



Technical Guideline TR-03105

Conformity Tests for Official Electronic ID Documents

Part 3.3: Test Plan for eID-Cards with
Advanced Security Mechanisms – EAC 2

Version 1.4

July 13rd, 2023



Version history

Version	Date	Editor	Description
0.30	12-10-2007	BSI/Networkers AG	EAC 2.0 conformity tests Proposal for harmonized document Working Draft
0.40	26-10-2007	BSI/Networkers AG	Editorial changes Additional test cases for layer 7
0.50	03-12-2007	BSI/Networkers AG	Editorial changes New test case definitions Including Comments from EAC 1.1 specification
0.60	18-01-2008	BSI/Networkers AG	Including changes from EAC 2.0 Public Beta 3
0.70	24-01-2008	BSI/Networkers AG	New test unit structure
0.80	23-10-2008	BSI/secunet AG	Including changes from EAC 1.12 and EAC 2.0 Almost Released
0.90	31-10-2008	BSI/secunet AG	Including changes from EAC 2.0 (Final)
1.00 beta 1	19-12-2008	BSI/secunet AG	Minor editorial changes
1.00 beta 2	20-02-2009	BSI/secunet AG	Resolved comments from DIF
1.00 beta 3	06-04-2009	BSI/secunet AG	Resolved comments from DIF
1.00 RC	06-12-2009	BSI/secunet AG	Resolved comments from DIF Including changes from EAC 2.02
1.00	24-02-2010	BSI/secunet AG	Resolved comments from DIF
1.01	2010-03-23	BSI	Minor editorial changes
1.02	2010-08-02	BSI	Correction in ISO chaining (PACE: General Authenticate command) Updated test case EAC2_DATA_A_3 for standardized domain parameters
1.03	2010-08-20	BSI	Test cases for layer 7 are updated for using standardized domain parameters

Version	Date	Editor	Description
			Minor updates on test cases EAC2_ISO7816_I_8, EAC2_ISO7816_L_15, EAC2_ISO7816_L_16, EAC2_ISO7816_L_19
			Minor updates on Certificates 9:10 AT_CERT_21 and AT_CERT_22
1.1 RC1	2018-01-19	BSI/secunet AG	Integrated Amendment Release 3
			Resolved comments
			Editorial changes
			Added new test suites for Manage Channel, Compare, Envelope/Get Response and CAv3
1.1 RC2	2018-04-30	BSI/secunet AG	Resolved comments of DIF AG Chip
1.1 RC3	2018-09-17	BSI/secunet AG	Resolved comments of DIF AG Chip
1.1 RC4	2018-11-22	BSI/secunet AG	Resolved comments of DIF AG Chip
			Handling of chips without CA-Infos in EF.CardAccess
1.1	2018-12-14	BSI	Resolution DIF AG Chip comments on RC 4
1.2 RC1	2019-10-11	BSI/secunet AG	Resolved comments of secunet
1.2 RC2	2019-12-16	BSI/secunet AG	Resolved comments of BSI and secunet
1.2 RC3	2020-01-08	BSI/secunet AG	Minor SM encoding fix
1.2	2020-02-10	BSI/secunet AG	Release
1.3 RC1	2023-02-23	BSI/secunet AG	Added Smart-eID (incl. Initial External Authentication and PACE-light aka CA+PA)
			Resolved comments of bdr, G+D, BSI
1.3 RC2	2023-04-19	BSI/secunet AG	Resolved comments of bdr, G+D, BSI
1.3 RC3	2023-05-02	BSI/secunet AG	Resolved comments of bdr, G+D, BSI
1.3 RC4	2023-05-10	BSI/secunet AG	Resolved comments of bdr, G+D, BSI
1.3	2023-05-15	BSI/secunet AG	Release
1.4	2023-07-13	BSI	Added CA+PA PIN Test cases

Test plan for eID-Cards with EAC 2.0

Version	Date	Editor	Description
			Resolved comments of bdr, G+D, BSI

Content

1 Introduction.....	17
1.1 Abbreviations.....	17
1.2 Reference documentation.....	18
1.3 Terminology.....	19
1.4 Test Coverage.....	20
1.4.1 MRTD with BAC and EAC 1.x.....	20
1.4.2 MRTD with PACE and EAC 1.x.....	21
1.4.3 eID-Card with EAC 2.x.....	21
1.4.4 ePassport Application Data Groups.....	21
1.4.5 eSign Application Data Groups.....	21
2 General test requirements.....	22
2.1 Test setup.....	22
2.2 Test profiles.....	22
2.2.1 Application Profiles.....	22
2.2.2 Protocol Profiles.....	23
2.2.3 Algorithm Profiles.....	25
2.2.4 Data Group Profiles.....	25
2.3 Key pair definition.....	26
2.4 Certificate specification.....	28
2.4.1 Certificate Set 1.....	28
2.4.2 Certificate Set 2.....	39
2.4.3 Certificate Set 3.....	42
2.4.4 Certificate Set 4.....	46
2.4.5 Certificate Set 5.....	48
2.4.6 Certificate Set 6.....	49
2.4.7 Certificate Set 7.....	56
2.4.8 Certificate Set 8.....	61
2.4.9 Certificate Set 9.....	64
2.4.10 Certificate Set 10.....	67
2.4.11 Certificate Set 11.....	72
2.4.12 Certificate Set 12.....	81
2.4.13 Certificate Set 13.....	94
2.4.14 Certificate Set 14.....	99
2.4.15 Certificate Set 15.....	103
2.4.16 Certificate Set 16.....	103
2.4.17 Certificate Set 17.....	103
2.4.18 Certificate Set 18.....	114

2.4.19 Certificate Set 19.....	118
2.4.20 Certificate Set 20.....	124
2.4.21 Certificate Set 21.....	129
2.4.22 Certificate Set 22.....	133
2.4.23 Certificate Set 23.....	136
2.4.24 Certificate Set 24.....	138
2.4.25 Certificate Set 25.....	140
2.4.26 Certificate Set 26.....	140
2.4.27 Certificate Set 27.....	140
2.4.28 Certificate Set 28.....	140
2.4.29 Certificate Set 29.....	141
2.4.30 Certificate Set 30.....	141
2.4.31 Certificate Set 31.....	146
2.4.32 Certificate Set 32.....	149
2.4.33 Certificate Set 33.....	168
3 Tests for layer 6 (ISO 7816).....	196
3.1 Test case notation.....	196
3.2 General requirements.....	196
3.2.1 Security Status.....	196
3.2.2 Extended length APDUs.....	197
3.2.3 Command Chaining.....	197
3.3 Unit test EAC2_ISO7816_H – Password Authenticated Connection Establishment (PACE).....	198
3.3.1 Test case EAC2_ISO7816_H_1.....	198
3.3.2 Test case EAC2_ISO7816_H_2.....	199
3.3.3 Test case EAC2_ISO7816_H_3.....	200
3.3.4 Test case EAC2_ISO7816_H_4_Template.....	201
3.3.5 Test case EAC2_ISO7816_H_5_Template.....	202
3.3.6 Test case EAC2_ISO7816_H_6_Template.....	203
3.3.7 Test case EAC2_ISO7816_H_7.....	205
3.3.8 Test case EAC2_ISO7816_H_8.....	205
3.3.9 Test case EAC2_ISO7816_H_9.....	205
3.3.10 Test case EAC2_ISO7816_H_10.....	205
3.3.11 Test case EAC2_ISO7816_H_11.....	205
3.3.12 Test case EAC2_ISO7816_H_12.....	205
3.3.13 Test case EAC2_ISO7816_H_13.....	205
3.3.14 Test case EAC2_ISO7816_H_14.....	206
3.3.15 Test case EAC2_ISO7816_H_15.....	206
3.3.16 Test case EAC2_ISO7816_H_16.....	206
3.3.17 Test case EAC2_ISO7816_H_17.....	206
3.3.18 Test case EAC2_ISO7816_H_18.....	206
3.3.19 Test case EAC2_ISO7816_H_19.....	206
3.3.20 Test case EAC2_ISO7816_H_20.....	206
3.3.21 Test case EAC2_ISO7816_H_21.....	206

3.3.22 Test case EAC2_ISO7816_H_22.....	206
3.3.23 Test case EAC2_ISO7816_H_23.....	207
3.3.24 Test case EAC2_ISO7816_H_24.....	207
3.3.25 Test case EAC2_ISO7816_H_25.....	207
3.3.26 Test case EAC2_ISO7816_H_26.....	207
3.3.27 Test case EAC2_ISO7816_H_27.....	207
3.3.28 Test case EAC2_ISO7816_H_28.....	207
3.3.29 Test case EAC2_ISO7816_H_29.....	208
3.3.30 Test case EAC2_ISO7816_H_30.....	208
3.3.31 Test case EAC2_ISO7816_H_31.....	208
3.3.32 Test case EAC2_ISO7816_H_32.....	208
3.3.33 Test case EAC2_ISO7816_H_33.....	208
3.3.34 Test case EAC2_ISO7816_H_34.....	209
3.3.35 Test case EAC2_ISO7816_H_35.....	209
3.3.36 Test case EAC2_ISO7816_H_36.....	210
3.3.37 Test case EAC2_ISO7816_H_37.....	211
3.4 Unit EAC2_ISO7816_I - Chip Authentication.....	212
3.4.1 Test case EAC2_ISO7816_I_1.....	212
3.4.2 Test case EAC2_ISO7816_I_2.....	213
3.4.3 Test case EAC2_ISO7816_I_3.....	214
3.4.4 Test case EAC2_ISO7816_I_4.....	215
3.4.5 Test case EAC2_ISO7816_I_5.....	216
3.4.6 Test case EAC2_ISO7816_I_6.....	217
3.4.7 Test case EAC2_ISO7816_I_7.....	217
3.4.8 Test case EAC2_ISO7816_I_8.....	218
3.4.9 Test case EAC2_ISO7816_I_9.....	219
3.4.10 Test case EAC2_ISO7816_I_10.....	220
3.4.11 Test case EAC2_ISO7816_I_11.....	221
3.4.12 Test case EAC2_ISO7816_I_12.....	222
3.4.13 Test case EAC2_ISO7816_I_13.....	223
3.4.14 Test case EAC2_ISO7816_I_14.....	224
3.4.15 Test case EAC2_ISO7816_I_15.....	224
3.4.16 Test case EAC2_ISO7816_I_16.....	225
3.4.17 Test case EAC2_ISO7816_I_17.....	226
3.5 Unit EAC2_ISO7816_J - Certificate verification.....	227
3.5.1 Test case EAC2_ISO7816_J_1_Template.....	228
3.5.2 Test case EAC2_ISO7816_J_2_Template.....	229
3.5.3 Test case EAC2_ISO7816_J_3_Template.....	230
3.5.4 Test case EAC2_ISO7816_J_4_Template.....	231
3.5.5 Test case EAC2_ISO7816_J_5_Template.....	232
3.5.6 Test case EAC2_ISO7816_J_6_Template.....	233
3.5.7 Test case EAC2_ISO7816_J_7_Template.....	234
3.5.8 Test case EAC2_ISO7816_J_8_Template.....	235
3.5.9 Test case EAC2_ISO7816_J_9_Template.....	237

Test plan for eID-Cards with EAC 2.0

3.5.10 Test case EAC2_ISO7816_J_10_Template.....	238
3.5.11 Test case EAC2_ISO7816_J_11.....	239
3.5.12 Test case EAC2_ISO7816_J_12_Template.....	241
3.5.13 Test case EAC2_ISO7816_J_13.....	242
3.5.14 Test case EAC2_ISO7816_J_14_Template.....	243
3.5.15 Test case EAC2_ISO7816_J_15_Template.....	243
3.5.16 Test case EAC2_ISO7816_J_16_Template.....	245
3.5.17 Test case EAC2_ISO7816_J_17_Template.....	246
3.5.18 Test case EAC2_ISO7816_J_18_Template.....	247
3.5.19 Test case EAC2_ISO7816_J_19_Template.....	248
3.5.20 Test case EAC2_ISO7816_J_20_Template.....	249
3.5.21 Test case EAC2_ISO7816_J_21_Template.....	250
3.5.22 Test case EAC2_ISO7816_J_22_Template.....	251
3.5.23 Test case EAC2_ISO7816_J_23_Template.....	253
3.5.24 Test case EAC2_ISO7816_J_24_Template.....	254
3.5.25 Test case EAC2_ISO7816_J_25_Template.....	255
3.5.26 Test case EAC2_ISO7816_J_26_Template.....	256
3.5.27 Test case EAC2_ISO7816_J_27_Template.....	257
3.5.28 Test case EAC2_ISO7816_J_28_Template.....	258
3.5.29 Test case EAC2_ISO7816_J_29_Template.....	260
3.5.30 Test case EAC2_ISO7816_J_30_Template.....	261
3.5.31 Test case EAC2_ISO7816_J_31_Template.....	262
3.5.32 Test case EAC2_ISO7816_J_32_Template.....	263
3.5.33 Test case EAC2_ISO7816_J_33_Template.....	264
3.5.34 Test case EAC2_ISO7816_J_34_Template.....	265
3.5.35 Test case EAC2_ISO7816_J_35_Template.....	267
3.5.36 Test case EAC2_ISO7816_J_36_Template.....	268
3.5.37 Test case EAC2_ISO7816_J_37_Template.....	269
3.5.38 Test case EAC2_ISO7816_J_38_Template.....	270
3.5.39 Test case EAC2_ISO7816_J_39_Template.....	271
3.5.40 Test case EAC2_ISO7816_J_40.....	273
3.5.41 Test case EAC2_ISO7816_J_41.....	273
3.5.42 Test case EAC2_ISO7816_J_42.....	274
3.5.43 Test case EAC2_ISO7816_J_43.....	275
3.5.44 Test case EAC2_ISO7816_J_44.....	276
3.5.45 Test case EAC2_ISO7816_J_45.....	277
3.5.46 Test case EAC2_ISO7816_J_46.....	278
3.5.47 Test case EAC2_ISO7816_J_47.....	279
3.5.48 Test case EAC2_ISO7816_J_48.....	280
3.5.49 Test case EAC2_ISO7816_J_49.....	282
3.5.50 Test case EAC2_ISO7816_J_50.....	283
3.5.51 Test case EAC2_ISO7816_J_51_Template.....	284
3.5.52 Test case EAC2_ISO7816_J_52_Template.....	285
3.6 Unit EAC2_ISO7816_K Terminal Authentication.....	286

3.6.1 Test case EAC2_ISO7816_K_1.....	287
3.6.2 Test case EAC2_ISO7816_K_2.....	288
3.6.3 Test case EAC2_ISO7816_K_3.....	290
3.6.4 Test case EAC2_ISO7816_K_4.....	291
3.6.5 Test case EAC2_ISO7816_K_5.....	292
3.6.6 Test case EAC2_ISO7816_K_6.....	293
3.6.7 Test case EAC2_ISO7816_K_7.....	295
3.6.8 Test case EAC2_ISO7816_K_8.....	296
3.6.9 Test case EAC2_ISO7816_K_9.....	298
3.6.10 Test case EAC2_ISO7816_K_10.....	299
3.6.11 Test case EAC2_ISO7816_K_11.....	301
3.6.12 Test case EAC2_ISO7816_K_12.....	302
3.6.13 Test case EAC2_ISO7816_K_13.....	304
3.6.14 Test case EAC2_ISO7816_K_14.....	305
3.6.15 Test case EAC2_ISO7816_K_15.....	307
3.6.16 Test case EAC2_ISO7816_K_16.....	308
3.7 Unit EAC2_ISO7816_L Effective Access Conditions.....	310
3.7.1 Test case EAC2_ISO7816_L_1.....	310
3.7.2 Test case EAC2_ISO7816_L_2.....	312
3.7.3 Test case EAC2_ISO7816_L_3.....	314
3.7.4 Test case EAC2_ISO7816_L_4.....	315
3.7.5 Test case EAC2_ISO7816_L_5.....	317
3.7.6 Test case EAC2_ISO7816_L_6.....	319
3.7.7 Test case EAC2_ISO7816_L_7.....	320
3.7.8 Test case EAC2_ISO7816_L_8.....	322
3.7.9 Test case EAC2_ISO7816_L_9.....	324
3.7.10 Test case EAC2_ISO7816_L_10.....	325
3.7.11 Test case EAC2_ISO7816_L_11.....	327
3.7.12 Test case EAC2_ISO7816_L_12.....	328
3.7.13 Test case EAC2_ISO7816_L_13 Template.....	330
3.7.14 Test case EAC2_ISO7816_L_14 Template.....	334
3.7.15 Test case EAC2_ISO7816_L_15 Template.....	337
3.7.16 Test case EAC2_ISO7816_L_16 Template.....	339
3.7.17 Test case EAC2_ISO7816_L_17.....	342
3.7.18 Test case EAC2_ISO7816_L_18.....	344
3.7.19 Test case EAC2_ISO7816_L_19.....	346
3.7.20 Test case EAC2_ISO7816_L_20.....	347
3.7.21 Test case EAC2_ISO7816_L_21.....	349
3.7.22 Test case EAC2_ISO7816_L_22.....	349
3.7.23 Test case EAC2_ISO7816_L_23.....	349
3.7.24 Test case EAC2_ISO7816_L_24.....	351
3.7.25 Test case EAC2_ISO7816_L_25.....	351
3.7.26 Test case EAC2_ISO7816_L_26.....	353
3.7.27 Test case EAC2_ISO7816_L_27.....	354

Test plan for eID-Cards with EAC 2.0

3.7.28 Test case EAC2_ISO7816_L_28.....	356
3.7.29 Test case EAC2_ISO7816_L_29.....	357
3.7.30 Test case EAC2_ISO7816_L_30.....	357
3.7.31 Test case EAC2_ISO7816_L_31.....	357
3.7.32 Test case EAC2_ISO7816_L_32.....	358
3.7.33 Test case EAC2_ISO7816_L_33.....	358
3.7.34 Test case EAC2_ISO7816_L_34.....	358
3.7.35 Test case EAC2_ISO7816_L_35.....	358
3.7.36 Test case EAC2_ISO7816_L_36.....	360
3.7.37 Test case EAC2_ISO7816_L_37.....	362
3.7.38 Test case EAC2_ISO7816_L_38.....	363
3.7.39 Test case EAC2_ISO7816_L_39.....	365
3.7.40 Test case EAC2_ISO7816_L_40.....	366
3.7.41 Test case EAC2_ISO7816_L_41.....	368
3.7.42 Test case EAC2_ISO7816_L_42.....	369
3.7.43 Test case EAC2_ISO7816_L_43.....	370
3.7.44 Test case EAC2_ISO7816_L_44.....	372
3.7.45 Test case EAC2_ISO7816_L_45.....	373
3.8 Unit EAC2_ISO7816_M Update mechanism.....	375
3.8.1 Test case EAC2_ISO7816_M_1_Template.....	375
3.8.2 Test case EAC2_ISO7816_M_2_Template.....	377
3.8.3 Test case EAC2_ISO7816_M_3_Template.....	378
3.8.4 Test case EAC2_ISO7816_M_4_Template.....	381
3.8.5 Test case EAC2_ISO7816_M_5_Template.....	382
3.8.6 Test case EAC2_ISO7816_M_6.....	384
3.8.7 Test case EAC2_ISO7816_M_7.....	384
3.8.8 Test case EAC2_ISO7816_M_8.....	386
3.8.9 Test case EAC2_ISO7816_M_9.....	387
3.8.10 Test case EAC2_ISO7816_M_10.....	387
3.8.11 Test case EAC2_ISO7816_M_11.....	388
3.8.12 Test case EAC2_ISO7816_M_12.....	389
3.8.13 Test case EAC2_ISO7816_M_13.....	390
3.8.14 Test case EAC2_ISO7816_M_14.....	390
3.9 Unit test EAC2_ISO7816_N – Migration policies.....	391
3.9.1 Test case EAC2_ISO7816_N_1.....	392
3.9.2 Test case EAC2_ISO7816_N_2.....	393
3.10 Unit EAC2_ISO7816_O Effective Access Conditions with PACE CHAT Restrictions.....	394
3.10.1 Test case EAC2_ISO7816_O_1.....	394
3.10.2 Test case EAC2_ISO7816_O_2.....	396
3.10.3 Test case EAC2_ISO7816_O_3.....	398
3.10.4 Test case EAC2_ISO7816_O_4.....	399
3.10.5 Test case EAC2_ISO7816_O_5 Template.....	401
3.10.6 Test case EAC2_ISO7816_O_6 Template.....	405

3.10.7 Test case EAC2_ISO7816_O_7 Template.....	408
3.10.8 Test case EAC2_ISO7816_O_8 Template.....	411
3.10.9 Test case EAC2_ISO7816_O_9.....	414
3.10.10 Test case EAC2_ISO7816_O_10.....	415
3.10.11 Test case EAC2_ISO7816_O_11.....	417
3.10.12 Test case EAC2_ISO7816_O_12.....	417
3.11 Unit test EAC2_ISO7816_P – PIN-Management.....	419
3.11.1 Test case EAC2_ISO7816_P_1.....	419
3.11.2 Test case EAC2_ISO7816_P_2.....	420
3.11.3 Test case EAC2_ISO7816_P_3.....	421
3.11.4 Test case EAC2_ISO7816_P_4.....	422
3.11.5 Test case EAC2_ISO7816_P_5.....	423
3.11.6 Test case EAC2_ISO7816_P_6.....	425
3.11.7 Test case EAC2_ISO7816_P_7.....	426
3.11.8 Test case EAC2_ISO7816_P_8.....	427
3.11.9 Test case EAC2_ISO7816_P_8a.....	429
3.11.10 Test case EAC2_ISO7816_P_9.....	429
3.11.11 Test case EAC2_ISO7816_P_10.....	430
3.11.12 Test case EAC2_ISO7816_P_11.....	431
3.11.13 Test case EAC2_ISO7816_P_12.....	432
3.11.14 Test case EAC2_ISO7816_P_13.....	433
3.11.15 Test case EAC2_ISO7816_P_14.....	434
3.11.16 Test case EAC2_ISO7816_P_15.....	435
3.11.17 Test case EAC2_ISO7816_P_16.....	436
3.11.18 Test case EAC2_ISO7816_P_17.....	436
3.11.19 Test case EAC2_ISO7816_P_18.....	437
3.11.20 Test case EAC2_ISO7816_P_19.....	437
3.11.21 Test case EAC2_ISO7816_P_20.....	437
3.11.22 Test case EAC2_ISO7816_P_21.....	438
3.11.23 Test case EAC2_ISO7816_P_22.....	439
3.12 Unit test EAC2_ISO7816_Q Auxiliary Data Verification.....	441
3.12.1 Test case EAC2_ISO7816_Q_1.....	441
3.12.2 Test case EAC2_ISO7816_Q_2.....	441
3.12.3 Test case EAC2_ISO7816_Q_3.....	442
3.12.4 Test case EAC2_ISO7816_Q_4.....	443
3.12.5 Test case EAC2_ISO7816_Q_5.....	443
3.12.6 Test case EAC2_ISO7816_Q_6.....	444
3.12.7 Test case EAC2_ISO7816_Q_7.....	444
3.12.8 Test case EAC2_ISO7816_Q_8.....	445
3.12.9 Test case EAC2_ISO7816_Q_9.....	445
3.12.10 Test case EAC2_ISO7816_Q_10.....	446
3.12.11 Test case EAC2_ISO7816_Q_11.....	446
3.12.12 Test case EAC2_ISO7816_Q_12.....	447
3.12.13 Test case EAC2_ISO7816_Q_13.....	447

Test plan for eID-Cards with EAC 2.0

3.12.14 Test case EAC2_ISO7816_Q_14.....	448
3.12.15 Test case EAC2_ISO7816_Q_15.....	448
3.12.16 Test case EAC2_ISO7816_Q_16.....	449
3.12.17 Test case EAC2_ISO7816_Q_17.....	449
3.12.18 Test case EAC2_ISO7816_Q_18.....	450
3.12.19 Test case EAC2_ISO7816_Q_19.....	451
3.12.20 Test case EAC2_ISO7816_Q_20.....	451
3.12.21 Test case EAC2_ISO7816_Q_21.....	452
3.12.22 Test case EAC2_ISO7816_Q_22.....	452
3.13 Unit test EAC2_ISO7816_R Restricted Identification.....	453
3.13.1 Test case EAC2_ISO7816_R_1.....	453
3.13.2 Test case EAC2_ISO7816_R_2.....	454
3.13.3 Test case EAC2_ISO7816_R_3.....	454
3.13.4 Test case EAC2_ISO7816_R_4.....	454
3.13.5 Test case EAC2_ISO7816_R_5.....	455
3.13.6 Test case EAC2_ISO7816_R_6.....	455
3.13.7 Test case EAC2_ISO7816_R_7.....	456
3.13.8 Test case EAC2_ISO7816_R_8.....	456
3.13.9 Test case EAC2_ISO7816_R_9.....	456
3.13.10 Test case EAC2_ISO7816_R_10.....	457
3.13.11 Test case EAC2_ISO7816_R_11.....	458
3.13.12 Test case EAC2_ISO7816_R_12.....	458
3.14 Unit test EAC2_ISO7816_T_Envelope mechanism.....	459
3.14.1 Test case EAC2_ISO7816_T_1_Template.....	459
3.14.2 Test case EAC2_ISO7816_T_2.....	461
3.14.3 Test case EAC2_ISO7816_T_3.....	461
3.14.4 Test case EAC2_ISO7816_T_4.....	462
3.14.5 Test case EAC2_ISO7816_T_5.....	462
3.15 Unit test EAC2_ISO7816_U_Compare.....	463
3.15.1 Test case EAC2_ISO7816_U_1_Template.....	463
3.15.2 Test case EAC2_ISO7816_U_2_Template.....	464
3.15.3 Test case EAC2_ISO7816_U_3_Template.....	466
3.15.4 Test case EAC2_ISO7816_U_4_Template.....	467
3.15.5 Test case EAC2_ISO7816_U_5_Template.....	469
3.15.6 Test case EAC2_ISO7816_U_6_Template.....	470
3.15.7 Test case EAC2_ISO7816_U_7_Template.....	471
3.15.8 Test case EAC2_ISO7816_U_8_Template.....	473
3.15.9 Test case EAC2_ISO7816_U_9.....	474
3.15.10 Test case EAC2_ISO7816_U_10.....	475
3.15.11 Test case EAC2_ISO7816_U_11.....	476
3.15.12 Test case EAC2_ISO7816_U_12.....	477
3.15.13 Test case EAC2_ISO7816_U_13.....	477
3.15.14 Test case EAC2_ISO7816_U_14.....	478

3.16 Unit test EAC2_ISO7816_V_Chip Authentication Version 3.....	478
3.16.1 Test case EAC2_ISO7816_V_1.....	479
3.16.2 Test case EAC2_ISO7816_V_2.....	480
3.16.3 Test case EAC2_ISO7816_V_3.....	481
3.16.4 Test case EAC2_ISO7816_V_4.....	482
3.16.5 Test case EAC2_ISO7816_V_5.....	483
3.16.6 Test case EAC2_ISO7816_V_6.....	484
3.16.7 Test case EAC2_ISO7816_V_7.....	485
3.16.8 Test case EAC2_ISO7816_V_8.....	485
3.16.9 Test case EAC2_ISO7816_V_9.....	486
3.16.10 Test case EAC2_ISO7816_V_10.....	487
3.16.11 Test case EAC2_ISO7816_V_11.....	487
3.16.12 Test case EAC2_ISO7816_V_12.....	489
3.17 Unit test EAC2_ISO7816_W_Initial External Authentication (IEA).....	490
3.17.1 Test case EAC2_ISO7816_W_1.....	490
3.17.2 Test case EAC2_ISO7816_W_2.....	490
3.17.3 Test case EAC2_ISO7816_W_3.....	491
3.17.4 Test case EAC2_ISO7816_W_4.....	492
3.17.5 Test case EAC2_ISO7816_W_5.....	492
3.17.6 Test case EAC2_ISO7816_W_6.....	493
3.17.7 Test case EAC2_ISO7816_W_7.....	493
3.17.8 Test case EAC2_ISO7816_W_8.....	494
3.17.9 Test case EAC2_ISO7816_W_9.....	495
3.17.10 Test case EAC2_ISO7816_W_10.....	495
3.17.11 Test case EAC2_ISO7816_W_11.....	496
3.17.12 Test case EAC2_ISO7816_W_12.....	496
3.17.13 Test case EAC2_ISO7816_W_13.....	497
3.17.14 Test case EAC2_ISO7816_W_14.....	497
3.17.15 Test case EAC2_ISO7816_W_15.....	498
3.18 Unit test EAC2_ISO7816_X_CA+PA.....	499
3.18.1 Test case EAC2_ISO7816_X_1.....	499
3.18.2 Test case EAC2_ISO7816_X_2.....	500
3.18.3 Test case EAC2_ISO7816_X_3.....	501
3.18.4 Test case EAC2_ISO7816_X_4.....	501
3.18.5 Test case EAC2_ISO7816_X_5.....	502
3.18.6 Test case EAC2_ISO7816_X_6.....	503
3.18.7 Test case EAC2_ISO7816_X_7.....	504
3.18.8 Test case EAC2_ISO7816_X_8.....	504
3.18.9 Test case EAC2_ISO7816_X_9.....	505
3.18.10 Test case EAC2_ISO7816_X_10.....	506
3.18.11 Test case EAC2_ISO7816_X_11.....	506
3.18.12 Test case EAC2_ISO7816_X_12.....	507
3.18.13 Test case EAC2_ISO7816_X_13.....	507

Test plan for eID-Cards with EAC 2.0

3.18.14 Test case EAC2_ISO7816_X_14.....	508
3.18.15 Test case EAC2_ISO7816_X_15.....	509
3.18.16 Test case EAC2_ISO7816_X_16.....	509
3.18.17 Test case EAC2_ISO7816_X_17.....	510
3.18.18 Test case EAC2_ISO7816_X_18.....	511
3.18.19 Test case EAC2_ISO7816_X_19.....	511
3.18.20 Test case EAC2_ISO7816_X_20.....	512
3.18.21 Test case EAC2_ISO7816_X_21.....	513
3.18.22 Test case EAC2_ISO7816_X_22.....	514
3.18.23 Test case EAC2_ISO7816_X_23.....	515
3.18.24 Test case EAC2_ISO7816_X_24.....	515
3.18.25 Test case EAC2_ISO7816_X_25.....	516
3.18.26 Test case EAC2_ISO7816_X_26.....	517
3.18.27 Test case EAC2_ISO7816_X_27.....	518
3.18.28 Test case EAC2_ISO7816_X_28.....	519
3.18.29 Test case EAC2_ISO7816_X_29.....	520
3.18.30 Test case EAC2_ISO7816_X_30.....	521
3.18.31 Test case EAC2_ISO7816_X_31.....	522
3.18.32 Test case EAC2_ISO7816_X_32.....	522
3.18.33 Test case EAC2_ISO7816_X_33.....	523
3.18.34 Test case EAC2_ISO7816_X_34.....	524
3.18.35 Test case EAC2_ISO7816_X_35.....	525
3.18.36 Test case EAC2_ISO7816_X_36.....	526
3.18.37 Test case EAC2_ISO7816_X_37.....	526
3.18.38 Test case EAC2_ISO7816_X_38.....	527
3.18.39 Test case EAC2_ISO7816_X_39.....	528
3.18.40 Test case EAC2_ISO7816_X_40.....	529
3.18.41 Test case EAC2_ISO7816_X_41.....	530
3.18.42 Test case EAC2_ISO7816_X_42.....	531
3.18.43 Test case EAC2_ISO7816_X_43.....	531
3.18.44 Test case EAC2_ISO7816_X_44.....	532
3.18.45 Test case EAC2_ISO7816_X_45.....	533
3.18.46 Test case EAC2_ISO7816_X_46.....	534
3.18.47 Test case EAC2_ISO7816_X_47.....	535
3.18.48 Test case EAC2_ISO7816_X_48.....	536
3.18.49 Test case EAC2_ISO7816_X_49.....	537
3.18.50 Test case EAC2_ISO7816_X_50.....	538
3.18.51 Test case EAC2_ISO7816_X_51.....	538
3.18.52 Test case EAC2_ISO7816_X_52.....	539
3.18.53 Test case EAC2_ISO7816_X_53.....	540
3.18.54 Test case EAC2_ISO7816_X_54.....	541
3.18.55 Test case EAC2_ISO7816_X_55.....	542
3.18.56 Test case EAC2_ISO7816_X_56.....	543
3.18.57 Test case EAC2_ISO7816_X_57.....	544
3.18.58 Test case EAC2_ISO7816_X_58.....	545

3.18.59 Test case EAC2_ISO7816_X_59.....	546
3.18.60 Test case EAC2_ISO7816_X_60.....	546
3.18.61 Test case EAC2_ISO7816_X_61.....	548
4 Tests for layer 7 (Data Structure).....	549
4.1 Unit EAC2_DATA_A, EF.CardAccess.....	549
4.1.1 Test case EAC2_DATA_A_1a.....	549
4.1.2 Test case EAC2_DATA_A_1b.....	550
4.1.3 Test case EAC2_DATA_A_2.....	550
4.1.4 Test case EAC2_DATA_A_3.....	551
4.1.5 Test case EAC2_DATA_A_4.....	551
4.1.6 Test case EAC2_DATA_A_5.....	552
4.1.7 Test case EAC2_DATA_A_6.....	553
4.1.8 Test case EAC2_DATA_A_7.....	553
4.1.9 Test case EAC2_DATA_A_8.....	553
4.1.10 Test case EAC2_DATA_A_9.....	553
4.1.11 Test case EAC2_DATA_A_10.....	554
4.1.12 Test case EAC2_DATA_A_11.....	554
4.1.13 Test case EAC2_DATA_A_12.....	555
4.2 Unit EAC2_DATA_B, EF.CardSecurity.....	555
4.2.1 Test case EAC2_DATA_B_1.....	555
4.2.2 Test cases EAC2_DATA_B_2 to EAC2_DATA_B_7.....	556
4.2.3 Test case EAC2_DATA_B_8.....	556
4.2.4 Test case EAC2_DATA_B_9.....	557
4.2.5 Test case EAC2_DATA_B_10.....	557
4.2.6 Test case EAC2_DATA_B_11.....	558
4.2.7 Test case EAC2_DATA_B_12.....	558
4.2.8 Test case EAC2_DATA_B_13.....	559
4.2.9 Test case EAC2_DATA_B_14.....	559
4.3 Unit EAC2_EIDDATA_B eID Data Groups.....	560
4.3.1 Test case EAC2_EIDDATA_B_1.....	560
4.3.2 Test case EAC2_EIDDATA_B_2.....	560
4.3.3 Test case EAC2_EIDDATA_B_3.....	560
4.3.4 Test case EAC2_EIDDATA_B_4.....	561
4.3.5 Test case EAC2_EIDDATA_B_5.....	561
4.3.6 Test case EAC2_EIDDATA_B_6.....	561
4.3.7 Test case EAC2_EIDDATA_B_7.....	562
4.3.8 Test case EAC2_EIDDATA_B_8.....	562
4.3.9 Test case EAC2_EIDDATA_B_9.....	562
4.3.10 Test case EAC2_EIDDATA_B_10.....	562
4.3.11 Test case EAC2_EIDDATA_B_11.....	563
4.3.12 Test case EAC2_EIDDATA_B_12.....	563
4.3.13 Test case EAC2_EIDDATA_B_13.....	563
4.3.14 Test case EAC2_EIDDATA_B_14.....	563

Test plan for eID-Cards with EAC 2.0

4.3.15 Test case EAC2_EIDDATA_B_15.....	564
4.3.16 Test case EAC2_EIDDATA_B_16.....	564
4.3.17 Test case EAC2_EIDDATA_B_17.....	564
4.3.18 Test case EAC2_EIDDATA_B_18.....	564
4.3.19 Test case EAC2_EIDDATA_B_19.....	565
4.3.20 Test case EAC2_EIDDATA_B_20.....	565
4.3.21 Test case EAC2_EIDDATA_B_21.....	565
4.3.22 Test case EAC2_EIDDATA_B_22.....	565
4.4 Unit EAC2_DATA_C, EF.ChipSecurity.....	566
4.4.1 Test case EAC2_DATA_C_1.....	566
4.4.2 Test cases EAC2_DATA_C_2 to EAC2_DATA_C_10.....	567
4.4.3 Test case EAC2_DATA_C_11.....	567
4.4.4 Test case EAC2_DATA_C_12.....	567
Annex A Implementation conformance statement.....	569
A.1 Supported profiles.....	569
A.2 Supported cryptographic algorithm.....	571
A.3 Cryptosystem migration policy.....	571
A.4 EF.CardSecurity information.....	571
A.5 Additional Information.....	573
A.6 PSA Information.....	573
A.7 Initial External Authentication Information.....	574

1 Introduction

The TR 03105 defines a RF protocol and application test standard for eID-Cards. Version 2.0 of that document includes security mechanisms for ePassport, eID and eSign applications.

This document describes the test plan for machine-readable travel documents (eMRTDs) with advanced security mechanisms used for ePassport, eID and eSign applications referring to EAC version 2 and the corresponding dependencies.

As already known by the EAC version 1 test plan, this specification has a layer based structure. The layers 1 - 4 refer the RF protocol according to the ISO/IEC 14443 1-4 standard. Since the defined security mechanisms have no direct influence on this abstraction layer, this amendment does not contain any tests for these layers.

However, this document concentrates on the tests for the layer 6 (ISO/IEC 7816) and 7 (data group encoding).

This document is heavily based on the AFNOR/BSI test plan for EAC-passports. Especially tests for Chip and Terminal Authentication as well as the certificate structure are adopted by that document.

1.1 Abbreviations

Abbreviation	Full name
ADH	Asynchronous Diffie-Hellman
AT	Authentication Template
BAC	Basic Access Control
CA	Chip Authentication (in MRTD security mechanism contexts) Certificate Authority (in certificate contexts)
CA+PA	Chip authenticated connection establishment including password authentication
CAN	Card Access Number
CAR	Certification Authority Reference
CHAT	Certificate Holder Authorization Template
CHR	Certificate Holder Reference
CSCA	Country Signing Certificate Authority
CV	Card Verifiable
CVCA	Country Verifying Certificate Authority
DDO	Discretionary Data Object
DG	Data Group
DO	Data Object
EAC	Extended Access Control
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
DH	Diffie-Hellman
DST	Digital Signature Template
DV	Document Verifier
ICS	Implementation Conformance Statement (see Annex A)
IEA	Initial External Authentication
IS	Inspection System

Abbreviation	Full name
LDS	Logical Data Structure
KAEG	Key Agreement ElGamal-type
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
MSE	Manage Security Environment
OID	Object Identifier
PACE	Password Authenticated Connection Establishment
PICC	Proximity Integrated Circuit Card
PIN	Personal Identification Number
PS	Pseudonymous Signature
PSA	Pseudonymous Signature for Authentication
PSO	Perform Security Operation
PUK	PIN Unblocking Key
RFU	Reserved for Future Use
RSA	Rivest Shamir Adleman
TA	Terminal Authentication

1.2 Reference documentation

The following documentation serves as a reference for this specification:

- [R1] ICAO Doc 9303, Seventh Edition, Part 10
- [R2] TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1: eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, March 2012
- [R3] RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997
- [R4] ISO/IEC 7816-4:2013. Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange
- [R5] PKCS #3: Diffie-Hellman Key-Agreement Standard, Version 1.4, November 1993
- [R6] TR-03111: Technical Guideline, Elliptic Curve Cryptography, Version 2.1, June 2018
- [R7] TR-03105: Technical Guideline, Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Version 1.1, July 2007, referencing EAC version 1.1
- [R8] TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3: Common Specifications, Version 2.21, December 2016
- [R9] BSI, AFNOR: TR-03105 Part 3.2. Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Tests for Security Implementation, Version 1.5, 2018
- [R10] RFC 3852, Housley, Russel, Cryptographic message syntax (CMS), RFC3852, 2004
- [R11] ANSI, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, ANSI X9.42-2000, 1999
- [R12] TR-03110-Amendment: Protocol extensions and specifications for Smart-eID

1.3 Terminology

The key words "MUST", "SHALL", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY" in this document are to be interpreted as described in [R3].

Key word	Description
MUST	This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
MUST NOT	This phrase, or the phrase „SHALL NOT“, means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications MUST be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications SHOULD be understood and the case carefully weighed before implementing any behavior described with this label.
MAY	This word, or the adjective „OPTIONAL“, means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

1.4 Test Coverage

The following figure shows the test coverage of the different test specifications.

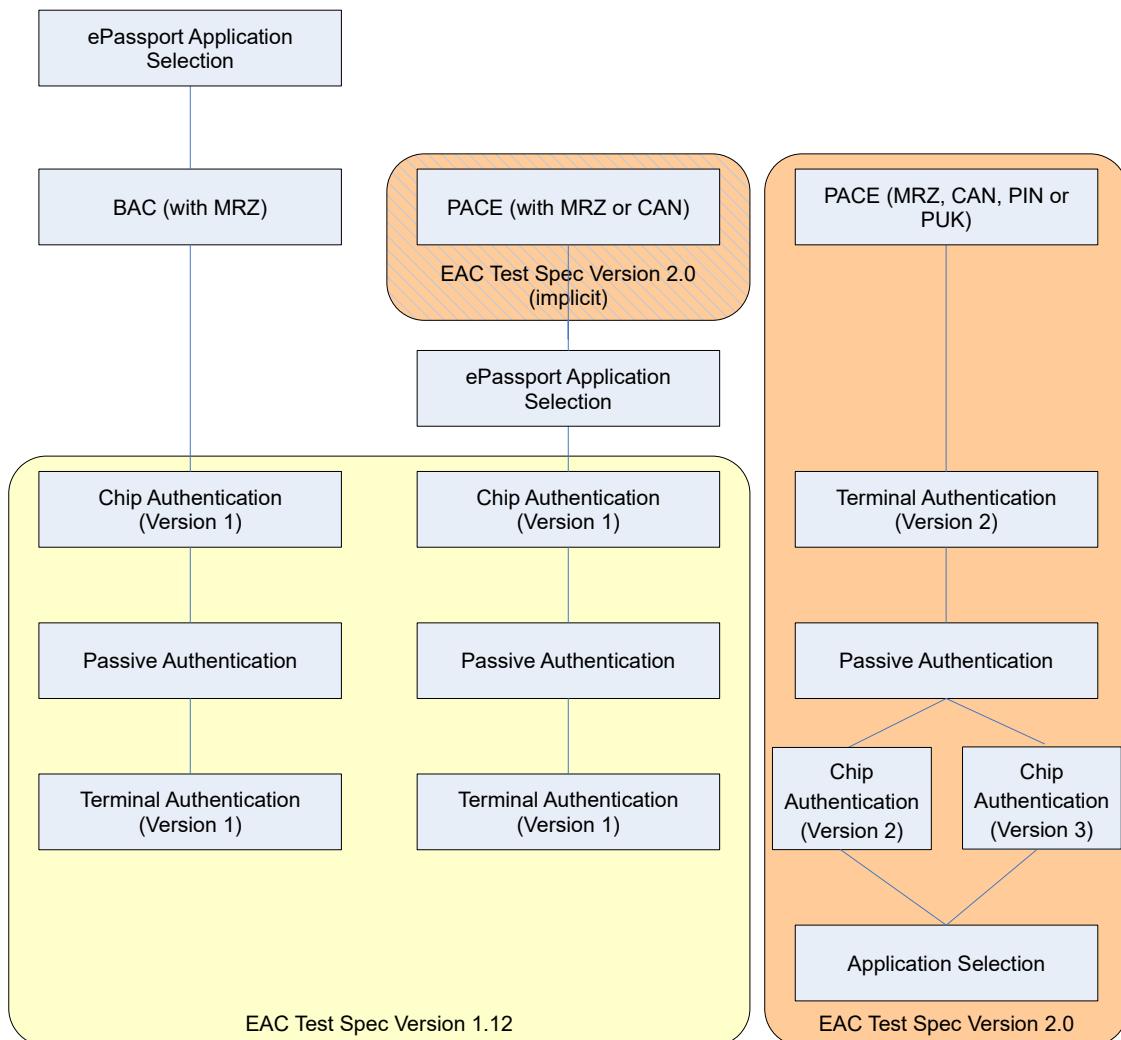


Figure 1: Test Coverage

The structure of the document is based on the EAC 1.11 test specification ([R9]). As far as possible identical unit names have been used for identical algorithm types, e.g. Chip Authentication is named as “Unit I” in this document as well as in the EAC 1.11 specification. The list of certificates is also based on the EAC 1.11 specification and extended by certificate types defined in the EAC 2.0 standard.

Three kinds of eID-Cards have to be observed as described below.

1.4.1 MRTD with BAC and FAC 1-x

If your MRTD is a BAC/EAC Version 1.x card please refer to [R9] only. There are no tests within this document that fit your needs.

1.4.2 MRTD with PACE and EAC 1.x

If your MRTD is an EAC Version 1.x card which also supports PACE, you have to perform the PACE tests defined here (see 3.3) and after that the following additional units of [R9]:

- ISO7816_H
- ISO7816_I
- ISO7816_J
- ISO7816_K
- ISO7816_L
- ISO7816_M

All test cases mentioned above have to be performed twice. In the first test run replace the precondition called “The BAC mechanism MUST/MUST NOT be performed” by “The PACE mechanism (with MRZ) MUST/MUST NOT be performed”. In the second test run replace the precondition called “The BAC mechanism MUST/MUST NOT be performed” by “The PACE mechanism (with CAN) MUST/MUST NOT be performed”.

Nevertheless PACE with EAC 1.x is not tested explicitly here.

1.4.3 eID-Card with EAC 2.x

If your MRTD is an eID-Card with EAC Version 2.x only, the test cases defined here have to be performed. If there are any references to other documents, they are described within the corresponding test unit.

1.4.4 ePassport Application Data Groups

The ePassport data groups are not tested within this specification.

1.4.5 eSign Application Data Groups

eSign is out of scope of both the EAC 1.x and EAC 2.x specification and therefore not tested here.

2 General test requirements

2.1 Test setup

For setting up these tests, any contactless reader supporting type A and type B protocols can be used. However, this reader has to support extended length APDUs requested for Terminal Authentication.

To execute any of the test cases described here, several types of test samples are required.

For executing all tests with one sample, this sample has to implement the ePassport application as defined by [R1], [R2] and [R8], the eID application as specified in [R9] and the eSign application for electronic signatures.

For executing separate tests of each application type one sample per application type is required (e.g. ePassport or eID card or eSign card). Cross-Application tests cannot be performed with these types of samples.

For executing cross-application mechanisms two types of samples are required: for executing read access tests to eID applications from ePassport application a sample with ePassport and eID application is necessary.

Some of the tests specified for layer 6 (ISO/IEC 7816) rely on the proper coding of the logical data structure stored in the chip. Therefore, it is RECOMMENDED that the layer 7 tests are performed before the layer 6 tests to detect coding related issues beforehand.

IMPORTANT NOTE: This test plan contains certain test cases, which verify the MRTD's behavior with expired certificates. During these tests, the effective date stored inside the chip is changed. Therefore a set of certificates can be used only once with a single card sample. After these tests have been performed, another sample or a new set of certificates is needed to repeat the tests.

This test plan also defines tests, which block or suspend PINs. After these tests have been performed, some of the features of the MRTD may be temporarily or permanently blocked or unusable.

Therefore, it is recommended to perform these tests as the last ones in a test sequence. If there is no way to unblock blocked or suspended PINs using PUKs or similar mechanisms, the vendor has to decide whether to perform or to skip these destructive tests.

2.2 Test profiles

This amendment defines several types of profiles. It is distinguished between “Application Profiles”, “Protocol Profiles”, “Algorithm Profiles” and “Data Group Profiles”. These types of profiles can be combined as defined by the corresponding card/application specification. Especially application profiles may include some implicit assumptions as defined in the corresponding specification (e.g. existence of PIN mechanisms when using eID application).

Profiles not mentioned within a test case MAY be present nevertheless (e.g. an eID application within ePassport tests). If the absence of a profile is necessary to fulfill the test case, it is separately mentioned in the test requirements.

2.2.1 Application Profiles

Profile-ID	Profile	Remark
ePassport	Electronic Passport Application	An application which contains data as specified in [R8] and [R1]. This profile implicitly includes usage of PACE with MRZ
eID	Electronic Identification	An application which contains data as specified in [R8]. This

Profile-ID	Profile	Remark
	Application	profile implicitly includes PIN/PUK management as defined in [R8].
eSign	Electronic Signature Application	An application which contains eSign specific data.
(NOT) Smart-eID	Smart eID	An eID application running on the Secure Element integrated in a smartphone or similar device.

2.2.2 Protocol Profiles

Profile-ID	Profile	Remark
PACE	Password Authenticated Connection Establishment	A MRTD which does not contain sensitive biometric data, like finger prints, can still use the Password Authenticated Connection Establishment mechanism to support strong communication encryption. This profile only covers version 2.
TA2	Terminal Authentication, Version 2	This profile is separated into two new profiles: TA2_IS and TA2_AT (see below).
CA2	Chip Authentication, Version 2	In addition to Terminal Authentication Chip authentication MUST be performed for all EAC version 2 capable MRTDs within the general authentication procedure. It supports chip cloning protection and strong communication encryption. This profile only covers version 2 Chip Authentication.
CA3	Chip Authentication, Version 3	This protocol is an alternative to the combination of Chip Authentication Version 2 and Restricted Identification (RI) providing additional features.
CA3_ReUse	Chip Authentication, Version 3 with Re-Use of PACE key	The ephemeral PACE-GM public key is reused by the chip during CA3.
MIG	Migration	According to the EAC specification the algorithm used for the Terminal Authentication process can be changed with an appropriate link certificate if the chip supports more than one algorithm. The tests for this Migration profile MUST only be performed, if the chip supports the migration from one cryptosystem to another. This must be stated in the ICS.
DATE	Date validation	Since the validation of the certificates effective and expiration date is not explicitly required by the EAC specification, the optional tests which belong to the Date validation profile must only be performed if this is supported by the chip. This must be stated in ICS.
RI	Restricted Identification	A MRTD which supports the Restricted Identification of terminals as specified in [R8].

Profile-ID	Profile	Remark
RI_DP	Restricted Identification Domain Parameters	As RI. The MRTD additionally provides an optional RestrictedIdentificationDomainParameterInfo data structure. According to EAC specification, this is optional and must be stated in ICS.
AUX	Auxiliary Data Verification	A MRTD which supports Auxiliary Data Verification mechanisms (age verification, document validity verification or Municipality ID verification) as specified in [R8].
(NOT) CNG_PIN_PUK	Change PIN using PACE with PUK	This profile allows a “Change PIN” procedure after PACE has been performed using PUK as authentication secret. Vice versa, if “Change PIN” procedure is NOT allowed, that profile is prefixed with NOT. According to EAC specification, this is optional and must be stated in ICS.
(NOT) CNG_PIN_AR	Change PIN allowed by Access Rights	This profile allows a “Change PIN” procedure for authentication terminals with “PIN Management” access right. Vice versa, if “Change PIN” procedure is NOT allowed, that profile is prefixed with NOT. According to EAC specification, this is optional and must be stated in ICS.
(NOT) CNG_CAN_AR	Change CAN allowed by Access Rights	This profile allows a “Change CAN” procedure for authentication terminals with “PIN Management” access right. Vice versa, if “Change CAN” procedure is NOT allowed, that profile is prefixed with NOT. According to EAC specification, this is optional and must be stated in ICS.
CS	Chip Security	A MRTD which stores a ChipSecurity file containing PrivilegedTerminalInfo with chip-individual keys and eIDSecurityInfo.
ENV	Envelope Mechanism	To support also terminals without extended length transport capability, chips can use the alternative Envelope mechanism.
CMP	Compare	The command Compare is used to verify authenticated auxiliary data.
AUTH_EXT	Authorization Extension	Authorization Extensions are special type of certificate extension. These extensions convey authorizations additional to those in the CHAT contained in the certificate.
BAC	Basic Access Control	According to ICAO Doc 9303 Part 11 starting on January 1st 2018 eMRTDs may support PACE only.
CSTA	EF.CardSecurity is protected by TA	EF.CardSecurity can be protected by PACE or by TA. Protection by TA was initially introduced in [R8] and protection by PACE was initially introduced in [R1].
PSAInfo	Use of PSAInfo	EF.CardAccess or EF.CardSecurity contains a PSAInfo element.
CardInfo	Use of CardInfo	EF.CardAccess or EF.CardSecurity contains a CardInfo element.

Profile-ID	Profile	Remark
PrivTerInfo	Use of PrivilegedTerminalInfo	EF.CardAccess or EF.CardSecurity contains a PrivilegedTerminalInfo element.
TA2_IS	Use of Terminal Authentication with IS certificates	To assure that Terminal Authentication v2 protocol is verified for both contexts, IS and AT, the profile TA2 is separated into two profiles. TA2_IS is relevant for eMRTD.
TA2_AT	Use of Terminal Authentication with AT certificates	To assure that Terminal Authentication v2 protocol is verified for both contexts, IS and AT, the profile TA2 is separated into two profiles. TA2_AT is relevant for eID and Smart-eID.
(NOT) CAPA	Use CA-PA instead of PACE	CA+PA aka PACE-light is introduced as an alternative to PACE for secure elements which lack the support for point addition on elliptic curves.

2.2.3 Algorithm Profiles

Profile-ID	Profile	Remark
DH	Diffie-Hellman	According to the EAC specification, the chip can support Diffie-Hellman or elliptic curve based Diffie-Hellman key agreement algorithms. Test cases which belong to the DH profile are only applicable if the DH algorithm is used.
ECDH	Elliptic Curve Diffie- Hellman	According to the EAC specification, the chip can support Diffie-Hellman or elliptic curve based Diffie-Hellman key agreement algorithms. Test cases which belong to the ECDH profile are only applicable if the elliptic curve based DH algorithm is used.
ECDSA	Elliptic curve algorithm	According to the EAC specification a chip is free to support either elliptic curve or RSA based keys. All tests which belong to the ECDSA profile MUST only be processed if the test object is personalized with elliptic curve based keys.
RSA	RSA algorithm	According to the EAC specification a chip is free to support either elliptic curve or RSA based keys. All tests which belong to the RSA profile MUST only be processed if the test object is personalized with RSA based keys.

2.2.4 Data Group Profiles

If there are any (optional) data groups that have to be present to perform the corresponding tests, these data groups are mentioned separately.

Profile-ID	Profile	Remark
DGx	Data Group x	Data group x must be present on the card

2.3 Key pair definition

The certificate sets defined in chapter 2.4 are based on several asymmetric key pairs. In preparation to the tests, these key pairs have to be generated. The parameter used for these keys are depending on the initial CVCA private keys.

The initial CVCA root private keys SHOULD be provided by the ePassport vendor. It is also possible the ePassport vendor generates all keys and certificates on its own and passes it to the test operator for the tests.

There are separate CVCA roots for each terminal type. These CVCA roots have different key pairs.

For the key set 13 (CVCA_KEY_13, DV_KEY_13, IS_KEY_13) the algorithm for the cryptosystem migration MUST be used as defined in the ICS.

All key pairs MUST be generated independently, so it is not permitted to use the same key pair for all sets.

Key pair	Description
CVCA_KEY_00	The key pair CV_KEY_00 is the public/private key for the initial CVCA root.
DV_KEY_01	Key pair of the test DV 01
IS_KEY_01	Key pair of the test IS 01
DV_KEY_02	Key pair of the test DV 02
IS_KEY_02	Key pair of the test IS 02
DV_KEY_03	Key pair of the test DV 03
IS_KEY_03	Key pair of the test IS 03
DV_KEY_04	Key pair of the test DV 04
IS_KEY_04	Key pair of the test IS 04
DV_KEY_05	Key pair of the test DV 05
IS_KEY_05	Key pair of the test IS 05
DV_KEY_06	Key pair of the test DV 06
IS_KEY_06	Key pair of the test IS 06
CVCA_KEY_07	Key pair of the test CVCA 07
DV_KEY_07	Key pair of the test DV 07
IS_KEY_07	Key pair of the test IS 07
CVCA_KEY_08	Key pair of the test CVCA 08
CVCA_KEY_09	Key pair of the test CVCA 09
DV_KEY_09	Key pair of the test DV 09
CVCA_KEY_10	Key pair of the test CVCA 10
DV_KEY_10	Key pair of the test DV 10
IS_KEY_10	Key pair of the test IS 10
CVCA_KEY_11	Key pair of the test CVCA 11
DV_KEY_11	Key pair of the test DV 11
IS_KEY_11	Key pair of the test IS 11
DV_KEY_12	Key pair of the test DV 12
CVCA_KEY_13	Key pair of the test CVCA 13
DV_KEY_13	Key pair of the test DV 13

Key pair	Description
IS_KEY_13	Key pair of the test IS 13
DV_KEY_14a	Key pair of the test DV 14 (length equal to CVCA Key length)
DV_KEY_14b	Key pair of the test DV 14 (MUST be shorter than CVCA Key length)
IS_KEY_14a	Key pair of the test IS 14 (length equal to CVCA Key length)
IS_KEY_14b	Key pair of the test IS 14 (MUST be shorter than CVCA Key length)
DV_KEY_15	Key pair of the test DV 15
IS_KEY_15	Key pair of the test IS 15
DV_KEY_16	Key pair of the test DV 16
IS_KEY_16	Key pair of the test IS 16
CVCA_KEY_17	The key pair CVCA_KEY_17 is the public/private key for the AT CVCA root
DV_KEY_17	Key pair of the test DV 17
AT_KEY_17	Key pair of the test AT 17
DV_KEY_18	Key pair of the test DV 18
AT_KEY_18	Key pair of the test AT 18
DV_KEY_19	Key pair of the test DV 19
AT_KEY_19	Key pair of the test AT 19
DV_KEY_20	Key pair of the test DV 20
AT_KEY_20	Key pair of the test AT 20
DV_KEY_21	Key pair of the test DV 21
AT_KEY_21	Key pair of the test AT 21
DV_KEY_22	Key pair of the test DV 22
AT_KEY_22	Key pair of the test AT 22
AT_CVCA_KEY_23a	Key pair of the test AT CVCA 23a
AT_CVCA_KEY_23b	Key pair of the test AT CVCA 23b
DV_KEY_23	Key pair of the test DV 23
DV_KEY_24	Key pair of the test DV 24
AT_KEY_24	Key pair of the test AT 24
DV_KEY_25	deleted in version 1.00 RC
IS_KEY_25	deleted in version 1.00 RC
DV_KEY_26	deleted in version 1.00 RC
IS_KEY_26	deleted in version 1.00 RC
DV_KEY_27	deleted in version 1.1
IS_KEY_27	deleted in version 1.1
DV_KEY_28	deleted in version 1.1
IS_KEY_28	deleted in version 1.1
DV_KEY_30	Key pair of the test DV 30
AT_KEY_30	Key pair of the test AT 30
DV_KEY_31	Key pair of the test DV 31
AT_KEY_31	Key pair of the test AT 31

Key pair	Description
DV_KEY_32	Key pair of the test DV_32
AT_KEY_32	Key pair of the test AT_32
AT_CVCA_KEY_32	Key pair of the test AT CVCA 32
DV_KEY_33	Key pair of the test DV_33
AT_KEY_33	Key pair of the test AT_33

2.4 Certificate specification

Since the advanced security mechanisms are using a certificate based authentication schema, it is necessary to provide a set of well prepared certificates in order to perform all tests.

This chapter defines the exact set of certificates referred in the tests. Besides the regular certificate chain, there is also the need for special encoded certificates.

The certificates are specified in two different ways. For provider of personalized passport samples, which do already have a preconfigured trust point based on their own CVCA key pair, the chapters below defines a set of certificates relative to the effective date ($CVCA_{eff}$) and expiration date($CVCA_{exp}$) of the given CVCA. The time span between $CVCA_{eff}$ and $CVCA_{exp}$ MUST be at least two month to allow proper adoption of the certificate time scheme defined below. The “current date” of the provided sample MUST be set to $CVCA_{eff}$ before the tests are started. The CVCA MUST NOT restrict authorization in any way, i.e. its Certificate Holder Authorization contains all rights. The provider of the sample or the test laboratory has to generate the corresponding certificate according to this specification based on the CVCA data.

There are separate CVCA roots for each terminal type, but they all SHOULD have equal effective and expiration dates.

If no preconfigured key pair is available or if the production process allows the use of an externally defined CVCA, a certificate set can be used which is defined as a “worked example” by this specification. This set is provided for ECDSA, RSA and RSAPSS based certificates and is defined in a full binary form with fixed keys and dates. It also includes a definition for an initial CVCA key pair and its effective and expiry dates.

2.4.1 Certificate Set 1

The certificate set consist of a regular certificate chain (DV -> IS) which is used for the positive tests regarding the certificate verification. Furthermore it contains variants of the original DV certificate to simulate a variety of certificate coding issues (missing elements, badly encoded dates ...).

2.4.1.1 DV_CERT_1

ID	DV_CERT_1
Purpose	This certificate is a regular DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.
Version	1.11
Referred by	Test case EAC2_ISO7816_I_1, Test case EAC2_ISO7816_I_2, Test case EAC2_ISO7816_I_3, Test case EAC2_ISO7816_I_4, Test case EAC2_ISO7816_I_5, Test case EAC2_ISO7816_I_6, Test case EAC2_ISO7816_I_7, Test case EAC2_ISO7816_I_8, Test case EAC2_ISO7816_I_9, Test case EAC2_ISO7816_I_10,

	<p>Test case EAC2_ISO7816_I_11, Test case EAC2_ISO7816_I_12, Test case EAC2_ISO7816_I_13, Test case EAC2_ISO7816_I_14, Test case EAC2_ISO7816_I_15, Test case EAC2_ISO7816_I_16, Test case EAC2_ISO7816_J_1, Test case EAC2_ISO7816_J_2, Test case EAC2_ISO7816_J_3, Test case EAC2_ISO7816_J_4, Test case EAC2_ISO7816_J_5, Test case EAC2_ISO7816_J_12, Test case EAC2_ISO7816_J_14, Test case EAC2_ISO7816_J_15, Test case EAC2_ISO7816_J_16, Test case EAC2_ISO7816_J_20, Test case EAC2_ISO7816_J_23, Test case EAC2_ISO7816_J_24, Test case EAC2_ISO7816_J_25, Test case EAC2_ISO7816_J_26, Test case EAC2_ISO7816_J_27, Test case EAC2_ISO7816_J_28, Test case EAC2_ISO7816_J_29, Test case EAC2_ISO7816_J_30, Test case EAC2_ISO7816_J_31, Test case EAC2_ISO7816_J_32, Test case EAC2_ISO7816_J_33, Test case EAC2_ISO7816_J_34, Test case EAC2_ISO7816_J_35, Test case EAC2_ISO7816_J_36, Test case EAC2_ISO7816_J_37, Test case EAC2_ISO7816_J_38, Test case EAC2_ISO7816_J_39, Test case EAC2_ISO7816_K_1, Test case EAC2_ISO7816_K_2, Test case EAC2_ISO7816_K_3, Test case EAC2_ISO7816_K_4, Test case EAC2_ISO7816_K_6, Test case EAC2_ISO7816_K_7, Test case EAC2_ISO7816_K_8, Test case EAC2_ISO7816_K_9, Test case EAC2_ISO7816_K_10, Test case EAC2_ISO7816_K_11, Test case EAC2_ISO7816_K_12, Test case EAC2_ISO7816_K_14, Test case EAC2_ISO7816_L_9, Test case EAC2_ISO7816_L_10, Test case EAC2_ISO7816_L_11, Test case EAC2_ISO7816_L_12</p> <p>The DV_CERT_1 SHOULD also be used for all other test cases that rely on an established EAC session to access DG3 and DG4 of ePassports.</p>
Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certification Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>
Parameter	Certification Authority Reference As defined by the CVCA

Certificate Holder Reference	DETTESTDVDE001
Certificate Holder Authorization	domestic DV, DG 3, DG 4
Certificate effective date	CVCA _{eff}
Certificate expiration date	CVCA _{eff} + 1 month
Public Key reference	Public key of key pair DV_KEY_01
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.1.2 DV_CERT_1a

ID	DV_CERT_1a														
Purpose	This certificate is similar to DV_CERT_1, but does not contain a Certificate Holder Authorization														
Version	1.11														
Referred by	Test case EAC2_ISO7816_J_6														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETTESTDVDE001</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>absent</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_01</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_00</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETTESTDVDE001	Certificate Holder Authorization	absent	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_01	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETTESTDVDE001														
Certificate Holder Authorization	absent														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_01														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.1.3 DV_CERT_1b

ID	DV_CERT_1b															
Purpose	This certificate is similar to DV_CERT_1, but does not contain a Certificate Effective Date															
Version	1.11															
Referred by	Test case EAC2_ISO7816_J_7															
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>															
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE001</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>domestic DV, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>absent</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_01</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_00</td> </tr> </table>		Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE001	Certificate Holder Authorization	domestic DV, DG 3, DG 4	Certificate effective date	absent	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_01	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA															
Certificate Holder Reference	DETESTDVDE001															
Certificate Holder Authorization	domestic DV, DG 3, DG 4															
Certificate effective date	absent															
Certificate expiration date	CVCA _{eff} + 1 month															
Public Key reference	Public key of key pair DV_KEY_01															
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00															

2.4.1.4 DV_CERT_1c

ID	DV_CERT_1c	
Purpose	This certificate is similar to DV_CERT_1, but does not contain a Certificate Expiration Date	
Version	1.11	
Referred by	Test case EAC2_ISO7816_J_8	
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00</p>	

	<pre> 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>
Parameter	Certification Authority Reference
	As defined by the CVCA
	Certificate Holder Reference
	DETESTDVDE001
	Certificate Holder Authorization
	domestic DV, DG 3, DG 4
	Certificate effective date

2.4.1.5 DV_CERT_1d

ID	DV CERT 1d
Purpose	This certificate is similar to DV_CERT_1, but contains a badly encoded Certificate Effective Date (Invalid BCD encoding)
Version	1.11
Referred by	Test case EAC2_ISO7816_J_9
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 0A 0B 0C 0D 0E 0F 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference </p>

	<p><i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE001
	Certificate Holder Authorization	domestic DV, DG 3, DG 4
	Certificate effective date	0A 0B 0C 0D 0E 0F (invalid BCD encoding)
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_01
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.1.6 DV_CERT_1e

ID	DV_CERT_1e	
Purpose	This certificate is similar to DV_CERT_1, but contains a badly encoded Certificate Expiration Date(Invalid BCD encoding)	
Version	1.11	
Referred by	Test case EAC2 ISO7816 J 10	
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 0A 0B 0C 0D 0E 0F 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	As defined by the CVCA

Certificate Holder Reference	DETESTDVDE001
Certificate Holder Authorization	domestic DV, DG 3, DG 4
Certificate effective date	CVCA _{eff}
Certificate expiration date	0A 0B 0C 0D 0E 0F (invalid BCD encoding)
Public Key reference	Public key of key pair DV_KEY_01
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.1.7 DV_CERT_1f

ID	DV_CERT_1f												
Purpose	This certificate is similar to DV_CERT_1, but contains a badly encoded Certificate Effective Date (Invalid Gregorian date)												
Version	1.11												
Referred by	Test case EAC2_ISO7816_J_17												
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>												
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE001</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>domestic DV, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>The month and the year used as defined by the CVCA_{eff} and the day is always set to the 32nd so that it becomes an invalid Gregorian date.</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{exp}</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_01</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE001	Certificate Holder Authorization	domestic DV, DG 3, DG 4	Certificate effective date	The month and the year used as defined by the CVCA _{eff} and the day is always set to the 32 nd so that it becomes an invalid Gregorian date.	Certificate expiration date	CVCA _{exp}	Public Key reference	Public key of key pair DV_KEY_01
Certification Authority Reference	As defined by the CVCA												
Certificate Holder Reference	DETESTDVDE001												
Certificate Holder Authorization	domestic DV, DG 3, DG 4												
Certificate effective date	The month and the year used as defined by the CVCA _{eff} and the day is always set to the 32 nd so that it becomes an invalid Gregorian date.												
Certificate expiration date	CVCA _{exp}												
Public Key reference	Public key of key pair DV_KEY_01												

	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
--	-----------------------	--

2.4.1.8 DV_CERT_1g

ID	DV_CERT_1g														
Purpose	This certificate is similar to DV_CERT_1, but contains a badly encoded Certificate Expiration Date (Invalid Gregorian date)														
Version	1.11														
Referred by	Test case EAC2 ISO7816_J_18														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE001</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>domestic DV, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>The month and the year used as defined by the CVCA_{eff} and the day is always set to the 32nd so that it becomes an invalid Gregorian date.</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_01</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_00</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE001	Certificate Holder Authorization	domestic DV, DG 3, DG 4	Certificate effective date	CVCA _{eff}	Certificate expiration date	The month and the year used as defined by the CVCA _{eff} and the day is always set to the 32 nd so that it becomes an invalid Gregorian date.	Public Key reference	Public key of key pair DV_KEY_01	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETESTDVDE001														
Certificate Holder Authorization	domestic DV, DG 3, DG 4														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	The month and the year used as defined by the CVCA _{eff} and the day is always set to the 32 nd so that it becomes an invalid Gregorian date.														
Public Key reference	Public key of key pair DV_KEY_01														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.1.9 DV_CERT_1h

ID	DV_CERT_1h														
Purpose	This certificate is similar to DV_CERT_1, but contains a Certificate Expiration Date BEFORE the Certificate Effective Date														
Version	1.11														
Referred by	Test case EAC2 ISO7816 J 19														
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>As defined by the CVCA</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTDVDE001</td></tr> <tr> <td>Certificate Holder Authorization</td><td>domestic DV, DG 3, DG 4</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff} + 1 day</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff}</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair DV_KEY_01</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_00</td></tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE001	Certificate Holder Authorization	domestic DV, DG 3, DG 4	Certificate effective date	CVCA _{eff} + 1 day	Certificate expiration date	CVCA _{eff}	Public Key reference	Public key of key pair DV_KEY_01	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETESTDVDE001														
Certificate Holder Authorization	domestic DV, DG 3, DG 4														
Certificate effective date	CVCA _{eff} + 1 day														
Certificate expiration date	CVCA _{eff}														
Public Key reference	Public key of key pair DV_KEY_01														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.1.10 DV_CERT_1i

ID	DV_CERT_1i
Purpose	This certificate is similar to DV_CERT_1, but contains a Certificate Holder Authorization with an invalid combination of OID (<id-AT>) and discretionary data object (structured like a relative authorization bit map for an IS)
Version	1.11

Referred by	Test case EAC2 ISO7816 J 21														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>As defined by the CVCA</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETTESTDVDE001</td></tr> <tr> <td>Certificate Holder Authorization</td><td>domestic DV, DG 3, DG 4</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 1 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair DV KEY_01</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_00</td></tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETTESTDVDE001	Certificate Holder Authorization	domestic DV, DG 3, DG 4	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV KEY_01	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETTESTDVDE001														
Certificate Holder Authorization	domestic DV, DG 3, DG 4														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV KEY_01														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.1.11 DV_CERT_1j

ID	DV_CERT_1j
Purpose	This certificate is similar to DV_CERT_1, but contains a Public Key with an invalid OID
Version	1.12
Referred by	Test case EAC2 ISO7816 J 22
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg</p>

	5F 24 06 hh 5F 37 ii jj
<p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference
	As defined by the CVCA
	Certificate Holder Reference
	DETESTDVDE001
	Certificate Public Key
	Bad OID (Use 0.4.0.127.0.7.2.2.2.5.1)
	Certificate Holder Authorization
	domestic DV, DG 3, DG 4
	Certificate effective date
	CVCA _{eff}
	Certificate expiration date
	CVCA _{eff} + 1 month
	Public Key reference
	Public key of key pair DV KEY_01
	Signing Key reference
	Signed with the private key of key pair CVCA KEY_00

2.4.1.12 IS_CERT_1

ID	IS_CERT_1
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_1
Version	1.11
Referred by	Test case EAC2_ISO7816_I_1, Test case EAC2_ISO7816_I_2, Test case EAC2_ISO7816_I_3, Test case EAC2_ISO7816_I_4, Test case EAC2_ISO7816_I_5, Test case EAC2_ISO7816_I_6, Test case EAC2_ISO7816_I_7, Test case EAC2_ISO7816_I_8, Test case EAC2_ISO7816_I_9, Test case EAC2_ISO7816_I_10, Test case EAC2_ISO7816_I_12, Test case EAC2_ISO7816_I_13, Test case EAC2_ISO7816_I_14, Test case EAC2_ISO7816_I_15, Test case EAC2_ISO7816_I_16, Test case EAC2_ISO7816_J_1, Test case EAC2_ISO7816_J_2, Test case EAC2_ISO7816_J_3, Test case EAC2_ISO7816_J_4, Test case EAC2_ISO7816_J_5, Test case EAC2_ISO7816_J_6, Test case EAC2_ISO7816_J_7, Test case EAC2_ISO7816_J_8, Test case EAC2_ISO7816_J_9, Test case EAC2_ISO7816_J_10, Test case EAC2_ISO7816_J_15, Test case EAC2_ISO7816_J_16, Test case EAC2_ISO7816_J_17, Test case EAC2_ISO7816_J_18, Test case EAC2_ISO7816_J_19, Test case EAC2_ISO7816_J_20, Test case EAC2_ISO7816_J_21, Test case EAC2_ISO7816_J_22, Test case EAC2_ISO7816_K_1, Test case EAC2_ISO7816_K_2, Test case EAC2_ISO7816_K_3,

	Test case EAC2_ISO7816_K_6, Test case EAC2_ISO7816_K_7, Test case EAC2_ISO7816_K_8, Test case EAC2_ISO7816_K_9, Test case EAC2_ISO7816_K_10, Test case EAC2_ISO7816_K_11, Test case EAC2_ISO7816_K_12, Test case EAC2_ISO7816_K_14, Test case EAC2_ISO7816_L_9, Test case EAC2_ISO7816_L_10, Test case EAC2_ISO7816_L_11, Test case EAC2_ISO7816_L_12														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>DETESTDVDE001</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTISDE001</td></tr> <tr> <td>Certificate Holder Authorization</td><td>IS, DG 3, DG 4</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 14 days</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair IS_KEY_01</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair DV_KEY_01</td></tr> </table>	Certification Authority Reference	DETESTDVDE001	Certificate Holder Reference	DETESTISDE001	Certificate Holder Authorization	IS, DG 3, DG 4	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 14 days	Public Key reference	Public key of key pair IS_KEY_01	Signing Key reference	Signed with the private key of key pair DV_KEY_01
Certification Authority Reference	DETESTDVDE001														
Certificate Holder Reference	DETESTISDE001														
Certificate Holder Authorization	IS, DG 3, DG 4														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 14 days														
Public Key reference	Public key of key pair IS_KEY_01														
Signing Key reference	Signed with the private key of key pair DV_KEY_01														
	Test case EAC2_ISO7816_K_6, Test case EAC2_ISO7816_K_7, Test case EAC2_ISO7816_K_8, Test case EAC2_ISO7816_K_9, Test case EAC2_ISO7816_K_10, Test case EAC2_ISO7816_K_11, Test case EAC2_ISO7816_K_12, Test case EAC2_ISO7816_K_14, Test case EAC2_ISO7816_L_9, Test case EAC2_ISO7816_L_10, Test case EAC2_ISO7816_L_11, Test case EAC2_ISO7816_L_12														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>DETESTDVDE001</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTISDE001</td></tr> <tr> <td>Certificate Holder Authorization</td><td>IS, DG 3, DG 4</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 14 days</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair IS_KEY_01</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair DV_KEY_01</td></tr> </table>	Certification Authority Reference	DETESTDVDE001	Certificate Holder Reference	DETESTISDE001	Certificate Holder Authorization	IS, DG 3, DG 4	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 14 days	Public Key reference	Public key of key pair IS_KEY_01	Signing Key reference	Signed with the private key of key pair DV_KEY_01
Certification Authority Reference	DETESTDVDE001														
Certificate Holder Reference	DETESTISDE001														
Certificate Holder Authorization	IS, DG 3, DG 4														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 14 days														
Public Key reference	Public key of key pair IS_KEY_01														
Signing Key reference	Signed with the private key of key pair DV_KEY_01														

2.4.2 Certificate Set 2

This certificate set contains certificates which are used to verify the behavior of ePassports in respect to foreign IS certificates.

2.4.2.1 DV_CERT_2

ID	DV_CERT_2
Purpose	This certificate is a regular foreign DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.
Version	1.11
Referred by	Test case EAC2_ISO7816_J_11

Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 43 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>As defined by the CVCA</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTDVDE002</td></tr> <tr> <td>Certificate Holder Authorization</td><td>foreign DV, DG 3, DG 4</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 1 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair DV_KEY_02</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_00</td></tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE002	Certificate Holder Authorization	foreign DV, DG 3, DG 4	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_02	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETESTDVDE002														
Certificate Holder Authorization	foreign DV, DG 3, DG 4														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_02														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.2.2 IS_CERT_2a

ID	IS_CERT_2a
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_2. It has an advanced effective date. (Beyond the expiration date of IS_CERT_2b).
Version	1.11
Referred by	Test case EAC2_ISO7816_J_11
Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</pre>

	<p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	DETESTDVDE002
	Certificate Holder Reference	DETESTISDE002
	Certificate Holder Authorization	IS, DG 3, DG 4
	Certificate effective date	CVCA _{eff} + 14 days
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair IS_KEY_02
	Signing Key reference	Signed with the private key of key pair DV_KEY_02

2.4.2.3 IS_CERT_2b

ID	IS_CERT_2b
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_2. It has an expiration date BEFORE the effective date of IS_CERT_2a.
Version	1.11
Referred by	Test case EAC2 ISO7816 J 11
Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object,</p>

	<i>jj</i> is the placeholder for the certificates signature (ii bytes)	
Parameter	Certification Authority Reference	DETESTDVDE002
	Certificate Holder Reference	DETESTISDE002
	Certificate Holder Authorization	IS, DG 3, DG 4
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 13 days
	Public Key reference	Public key of key pair IS_KEY_02
	Signing Key reference	Signed with the private key of key pair DV_KEY_02

2.4.3 Certificate Set 3

The certificate set follows a certification scheme where the DV permits full access to data group 3 and 4 while the IS certificate restricts the access to specific data group.

2.4.3.1 DV_CERT_3

ID	DV_CERT_3						
Purpose	This certificate is a regular DV certificate, with access rights for both data group 3 and 4.						
Version	1.11						
Referred by	Test case EAC2_ISO7816_L_1, Test case EAC2_ISO7816_L_2, Test case EAC2_ISO7816_L_3, Test case EAC2_ISO7816_L_4, Test case EAC2_ISO7816_O_1, Test case EAC2_ISO7816_O_2						
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>						
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE003</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>domestic DV, DG 3, DG 4</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE003	Certificate Holder Authorization	domestic DV, DG 3, DG 4
Certification Authority Reference	As defined by the CVCA						
Certificate Holder Reference	DETESTDVDE003						
Certificate Holder Authorization	domestic DV, DG 3, DG 4						

Certificate effective date	CVCA _{eff}
Certificate expiration date	CVCA _{eff} + 1 month
Public Key reference	Public key of key pair DV_KEY_03
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.3.2 DV_CERT_3a

ID	DV CERT 3a														
Purpose	This certificate is a regular DV certificate, with access rights for both data group 3 and 4. It is a copy of DV_CERT_3 with the exception that all RFU bits within CHAT are set to 1.														
Version	EAC2 1.0														
Referred by	Test case EAC2_ISO7816_L_35														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 BF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE003</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>domestic DV, DG 3, DG 4, RFU=1</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_03</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_00</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE003	Certificate Holder Authorization	domestic DV, DG 3, DG 4, RFU=1	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_03	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETESTDVDE003														
Certificate Holder Authorization	domestic DV, DG 3, DG 4, RFU=1														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_03														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.3.3 IS_CERT_3a

ID	IS_CERT_3a
----	------------

Test plan for eID-Cards with EAC 2.0

Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_3. It encodes access rights for data group 3 only.														
Version	1.11														
Referred by	Test case EAC2_ISO7816_K_13, Test case EAC2_ISO7816_K_14, Test case EAC2_ISO7816_K_15, Test case EAC2_ISO7816_L_1, Test case EAC2_ISO7816_L_2, Test case EAC2_ISO7816_M_6, Test case EAC2_ISO7816_O_1														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 01 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>DETESTDVDE003</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTISDE003</td></tr> <tr> <td>Certificate Holder Authorization</td><td>IS, DG 3</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 1 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair IS_KEY_03</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair DV_KEY_03</td></tr> </table>	Certification Authority Reference	DETESTDVDE003	Certificate Holder Reference	DETESTISDE003	Certificate Holder Authorization	IS, DG 3	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair IS_KEY_03	Signing Key reference	Signed with the private key of key pair DV_KEY_03
Certification Authority Reference	DETESTDVDE003														
Certificate Holder Reference	DETESTISDE003														
Certificate Holder Authorization	IS, DG 3														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair IS_KEY_03														
Signing Key reference	Signed with the private key of key pair DV_KEY_03														

2.4.3.4 IS_CERT_3b

ID	IS_CERT_3b
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_3. It encodes access rights for data group 4 only.
Version	1.11
Referred by	
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd</p>

	<pre> 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 02 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes) </p>
Parameter	Certification Authority Reference
	DETESTDVDE003
	Certificate Holder Reference
	DETESTISDE003
	Certificate Holder Authorization
	IS, DG 4
	Certificate effective date

2.4.3.5 IS_CERT_3c

ID	IS_CERT_3c
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_3. It encodes access rights for data group 3 only. It is a copy of IS_CERT_3a with the exception that all RFU bits within CHAT are set to 1.
Version	EAC2 1.0
Referred by	Test case EAC2 ISO7816 L 35
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 3D 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) </p>

	ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)	
Parameter	Certification Authority Reference	DETESTDVDE003
	Certificate Holder Reference	DETESTISDE003
	Certificate Holder Authorization	IS, DG 3, RFU=1
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair IS_KEY_03
	Signing Key reference	Signed with the private key of key pair DV_KEY_03

2.4.4 Certificate Set 4

The certificate set follows a certification scheme where the DV permits only access to data group 3 while the IS certificate permits full access to data group 3 and 4.

2.4.4.1 DV_CERT_4

ID	DV_CERT_4
Purpose	This certificate is a regular DV certificate, with access rights for group 3 only.
Version	1.11
Referred by	Test case EAC2_ISO7816_L_5, Test case EAC2_ISO7816_L_6, Test case EAC2_ISO7816_O_3
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 81 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate </p>

	<i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (<i>ii</i> bytes)	
Parameter	Certification Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE004
	Certificate Holder Authorization	domestic DV, DG 3
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair DV KEY_04
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.4.2 IS_CERT_4

ID	IS_CERT_4													
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_4. It encodes access rights for data group 3 and data group 4.													
Version	1.11													
Referred by	Test case EAC2_ISO7816_L_5, Test case EAC2_ISO7816_L_6, Test case EAC2_ISO7816_O_3													
Content definition	<p> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </p> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (<i>cc</i> bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (<i>ee</i> bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (<i>xx</i> bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (<i>ii</i> bytes) </p>													
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTDVDE004</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTISDE004</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>IS, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair IS_KEY_04</td> </tr> </table>		Certification Authority Reference	DETESTDVDE004	Certificate Holder Reference	DETESTISDE004	Certificate Holder Authorization	IS, DG 3, DG 4	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair IS_KEY_04
Certification Authority Reference	DETESTDVDE004													
Certificate Holder Reference	DETESTISDE004													
Certificate Holder Authorization	IS, DG 3, DG 4													
Certificate effective date	CVCA _{eff}													
Certificate expiration date	CVCA _{eff} + 1 month													
Public Key reference	Public key of key pair IS_KEY_04													

	Signing Key reference	Signed with the private key of key pair DV_KEY_04
--	-----------------------	---

2.4.5 Certificate Set 5

The certificate set follows a certification scheme where the DV permits only access to data group 4 while the IS certificate permits full access to data group 3 and 4.

2.4.5.1 DV_CERT_5

ID	DV_CERT_5														
Purpose	This certificate is a regular DV certificate, with access rights for group 4 only.														
Version	1.11														
Referred by	Test case EAC2_ISO7816_L_7, Test case EAC2_ISO7816_L_8, Test case EAC2_ISO7816_O_4														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 82 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE005</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>domestic DV, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_05</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_00</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE005	Certificate Holder Authorization	domestic DV, DG 4	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_05	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETESTDVDE005														
Certificate Holder Authorization	domestic DV, DG 4														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_05														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.5.2 IS_CERT_5

ID	IS_CERT_5
----	-----------

Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_5. It encodes access rights for data group 3 and data group 4.														
Version	1.11														
Referred by	Test case EAC2_ISO7816_L_7, Test case EAC2_ISO7816_L_8, Test case EAC2_ISO7816_O_4														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>DETTESTDVDE005</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETTESTISDE005</td></tr> <tr> <td>Certificate Holder Authorization</td><td>IS, DG 3, DG 4</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 1 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair IS_KEY_05</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair DV_KEY_05</td></tr> </table>	Certification Authority Reference	DETTESTDVDE005	Certificate Holder Reference	DETTESTISDE005	Certificate Holder Authorization	IS, DG 3, DG 4	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair IS_KEY_05	Signing Key reference	Signed with the private key of key pair DV_KEY_05
Certification Authority Reference	DETTESTDVDE005														
Certificate Holder Reference	DETTESTISDE005														
Certificate Holder Authorization	IS, DG 3, DG 4														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair IS_KEY_05														
Signing Key reference	Signed with the private key of key pair DV_KEY_05														

2.4.6 Certificate Set 6

This certificate set contains certificate which have different effective and expiration dates to test the ePassports behavior in respect to the update of the effective date and with expired certificates.

2.4.6.1 DV_CERT_6

ID	DV_CERT_6
Purpose	This certificate is a domestic DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.
Version	1.11
Referred by	Test case EAC2_ISO7816_M_1, Test case EAC2_ISO7816_M_2

Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>
Parameter	Certification Authority Reference
	As defined by the CVCA
	Certificate Holder Reference
	DETESTDVDE006
	Certificate Holder Authorization
	domestic DV, DG 3, DG 4
	Public Key reference

2.4.6.2 DV_CERT_6a

ID	DV_CERT_6a
Purpose	This DV certificate is similar to DV_CERT_6, but the certificate effective date is beyond the DV CERT_6 expiration date.
Version	1.11
Referred by	Test case EAC2_ISO7816 M 2
Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</pre>

	<p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE006
	Certificate Holder Authorization	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA _{eff} + 1 month + 1 day
	Certificate expiration date	CVCA _{eff} + 2 month
	Public Key reference	Public key of key pair DV KEY_06
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.6.3 IS_CERT_6a

ID	IS_CERT_6a
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_6. This IS certificate has an advanced effective date. (Beyond the expiration date of IS_CERT_6b)
Version	1.11
Referred by	Test case EAC2_ISO7816_M_1
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate</p>

	<i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (<i>ii</i> bytes)	
Parameter	Certification Authority Reference	DETESTDVDE006
	Certificate Holder Reference	DETESTISDE006
	Certificate Holder Authorization	IS, DG 3, DG 4
	Certificate effective date	CVCA _{eff} + 14 days
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair IS_KEY_06
	Signing Key reference	Signed with the private key of key pair DV_KEY_06

2.4.6.4 IS_CERT_6b

ID	IS_CERT_6b	
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_6. This IS certificate has an expiration date BEFORE the effective date of IS_CERT_6a.	
Version	1.11	
Referred by	Test case EAC2_ISO7816_M_1	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (<i>cc</i> bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (<i>ee</i> bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (<i>xx</i> bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (<i>ii</i> bytes)</p>	
Parameter	Certification Authority Reference Certificate Holder Reference Certificate Holder Authorization Certificate effective date Certificate expiration date Public Key reference Signing Key reference	
	DETESTDVDE006 DETESTISDE006 IS, DG 3, DG 4 CVCA _{eff} CVCA _{eff} + 13 days Public key of key pair IS_KEY_06 Signed with the private key of key pair DV_KEY_06	

2.4.6.5 DV_CERT_6b

ID	DV_CERT_6b														
Purpose	This certificate is a domestic DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits access to all eID special functions.														
Version	Smart-eID														
Referred by	Test case EAC2_ISO7816_M_1, Test case EAC2_ISO7816_M_2														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 40 40 00 00 FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the initial AT CVCA reference</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE006</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Domestic DV, eID-Specials (all)</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_6</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_17</td> </tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTDVDE006	Certificate Holder Authorization	Domestic DV, eID-Specials (all)	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_6	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
Certification Authority Reference	As defined by the initial AT CVCA reference														
Certificate Holder Reference	DETESTDVDE006														
Certificate Holder Authorization	Domestic DV, eID-Specials (all)														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_6														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17														

2.4.6.6 DV_CERT_6c

ID	DV_CERT_6c
Purpose	This DV certificate is similar to DV_CERT_6b, but the certificate effective date is beyond the DV_CERT_6b expiration date.
Version	Smart-eID

Test plan for eID-Cards with EAC 2.0

Referred by	Test case EAC2 ISO7816 M 2														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 40 40 00 00 FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>As defined by the initial AT CVCA reference</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTDVDE006</td></tr> <tr> <td>Certificate Holder Authorization</td><td>Domestic DV, eID-Specials (all)</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff} + 1 month + 1 day</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 2 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair DV KEY_06a</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_17</td></tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTDVDE006	Certificate Holder Authorization	Domestic DV, eID-Specials (all)	Certificate effective date	CVCA _{eff} + 1 month + 1 day	Certificate expiration date	CVCA _{eff} + 2 month	Public Key reference	Public key of key pair DV KEY_06a	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
Certification Authority Reference	As defined by the initial AT CVCA reference														
Certificate Holder Reference	DETESTDVDE006														
Certificate Holder Authorization	Domestic DV, eID-Specials (all)														
Certificate effective date	CVCA _{eff} + 1 month + 1 day														
Certificate expiration date	CVCA _{eff} + 2 month														
Public Key reference	Public key of key pair DV KEY_06a														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17														

2.4.6.7 AT_CERT_6c

ID	AT_CERT_6c
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_6b. This AT certificate has an advanced effective date. (Beyond the expiration date of AT_CERT_6d).
Version	Smart-eID
Referred by	Test case EAC2 ISO7816 M 1
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00</p>

	<pre> 00 00 00 04 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> 65 <i>kk</i> 73 L₇₃ 06 09 04 00 7F 00 07 03 01 03 02 80 11 <i>mm</i> 5F 37 <i>ii jj</i> </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>kk</i> is the encoded length of the certificate extension object, <i>ll</i> is the encoded length of the terminal sector hash <i>mm</i> is the placeholder for the terminal sector hash </p>
Parameter	Certification Authority Reference
	DETESTDVDE006
	Certificate Holder Reference
	DETESTATDE006
	Certificate Holder Authorization
	Authentication Terminal
	Certificate effective date

2.4.6.8 AT_CERT_6d

ID	AT_CERT_6d
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_6b. This AT certificate has an expiration date BEFORE the effective date of AT_CERT_6c.
Version	Smart-eID
Referred by	Test case EAC2_ISO7816_M_1
Content definition	<pre> 7F 21 <i>aa</i> 7F 4E <i>bb</i> 5F 29 01 00 42 <i>cc dd</i> 7F 49 <i>ee ff</i> 5F 20 <i>xx yy</i> 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 00 04 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> 65 <i>kk</i> 73 L₇₃ 06 09 04 00 7F 00 07 03 01 03 02 80 11 </pre>

	mm 5F 37 ii jj
<p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>kk</i> is the encoded length of the certificate extension object, <i>ll</i> is the encoded length of the terminal sector hash <i>mm</i> is the placeholder for the terminal sector hash </p>	
Parameter	Certification Authority Reference
	DETESTDVDE006
	Certificate Holder Reference
	DETESTATDE006
	Certificate Holder Authorization
	Authentication Terminal
	Certificate effective date
	CVCA _{eff}
	Certificate expiration date
	CVCA _{eff} + 13 days
	Public Key reference
	Public key of key pair AT_KEY_6
	Signing Key reference
	Signed with the private key of key pair DV_KEY_6

2.4.7 Certificate Set 7

This certificate set defines a link certificate used for the tests about the trust point update mechanism.

2.4.7.1 LINK_CERT_7

Note for ECDSA profile: Since the cryptographic mechanism is not changed by this link certificate it must be stated by the vendor of the test sample if the domain parameters should be included in this certificate (see ICS A).

ID	LINK CERT 7
Purpose	This certificate is a link certificate, which validity period starts one day before the original CVCA certificate expires.
Version	1.11
Referred by	Test case EAC2 ISO7816 M 3
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd

	<pre> 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3 5F 25 06 gg 5F 24 06 hh optional: 65 vv ww 5F 37 ii jj </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>vv</i> is the encoded length of the certificate extension, <i>ww</i> is the placeholder for the certificate extension (vv bytes)</p>																
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>As defined by the CVCA</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETTESTLINKDE007</td></tr> <tr> <td>Certificate Holder Authorization</td><td>CVCA, DG 3, DG 4</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{exp} - 1 day</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{exp} + 2 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair CVCA_KEY_07</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_00</td></tr> <tr> <td>Certificate Extension</td><td>As defined by the CVCA</td></tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETTESTLINKDE007	Certificate Holder Authorization	CVCA, DG 3, DG 4	Certificate effective date	CVCA _{exp} - 1 day	Certificate expiration date	CVCA _{exp} + 2 month	Public Key reference	Public key of key pair CVCA_KEY_07	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00	Certificate Extension	As defined by the CVCA
Certification Authority Reference	As defined by the CVCA																
Certificate Holder Reference	DETTESTLINKDE007																
Certificate Holder Authorization	CVCA, DG 3, DG 4																
Certificate effective date	CVCA _{exp} - 1 day																
Certificate expiration date	CVCA _{exp} + 2 month																
Public Key reference	Public key of key pair CVCA_KEY_07																
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00																
Certificate Extension	As defined by the CVCA																

2.4.7.2 LINK_CERT_7a

ID	LINK_CERT_7a
Purpose	This certificate is a link certificate, which validity period starts one day before the original CVCA certificate expires.
Version	Smart-eID
Referred by	Test case EAC2_ISO7816_M_3
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 05 40 40 00 </pre>

	00 FF 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> <i>optional:</i> 65 <i>vv</i> <i>ww</i> 5F 37 <i>ii jj</i> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>vv</i> is the encoded length of the certificate extension, <i>ww</i> is the placeholder for the certificate extension (vv bytes)</p>
Parameter	Certification Authority Reference
	As defined by the CVCA
	Certificate Holder Reference
	DETESTLINKDE007
	Certificate Holder Authorization
	CVCA, all eID functions
	Certificate effective date
	CVCA _{exp} - 1 day

2.4.7.3 DV_CERT_7a

ID	DV_CERT_7a
Purpose	This certificate is a domestic DV certificate, which was issued by the original CVCA.
Version	1.11
Referred by	Test case EAC2_ISO7816_M_3
Content definition	7F 21 <i>aa</i> 7F 4E <i>bb</i> 5F 29 01 00 42 <i>cc dd</i> 7F 49 <i>ee ff</i> 5F 20 <i>xx yy</i> 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> 5F 37 <i>ii jj</i> <p><i>aa</i> is the encoded combined length of certificate body and signature objects</p>

	<p><i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	As defined by the original CVCA
	Certificate Holder Reference	DETESTDVDE007
	Certificate Holder Authorization	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{exp}
	Public Key reference	Public key of key pair DV_KEY_07
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.7.4 DV_CERT_7b

ID	DV_CERT_7b
Purpose	This certificate is a domestic DV certificate, which was issued by the update CVCA (LINK_CERT_7).
Version	1.11
Referred by	Test case EAC2 ISO7816 M 3, Test case EAC2 ISO7816 M 8
Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object,</p>

	<i>jj</i> is the placeholder for the certificates signature (ii bytes)	
Parameter	Certification Authority Reference	DETESTLINKDE007
	Certificate Holder Reference	DETESTDVDE007
	Certificate Holder Authorization	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA _{exp} + 1 day
	Certificate expiration date	CVCA _{exp} + 1 month
	Public Key reference	Public key of key pair DV_KEY_07
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_07

2.4.7.5 DV_CERT_7c

ID	DV_CERT_7b												
Purpose	This certificate is a domestic DV certificate, which was issued by the original CVCA.												
Version	1.11												
Referred by	Test case EAC2_ISO7816_M_3												
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 05 00 00 00 00 04 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>												
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>As defined by the original CVCA</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTDVDE007</td></tr> <tr> <td>Certificate Holder Authorization</td><td>Domestic DV</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{exp}</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair DV_KEY_07a</td></tr> </table>	Certification Authority Reference	As defined by the original CVCA	Certificate Holder Reference	DETESTDVDE007	Certificate Holder Authorization	Domestic DV	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{exp}	Public Key reference	Public key of key pair DV_KEY_07a
Certification Authority Reference	As defined by the original CVCA												
Certificate Holder Reference	DETESTDVDE007												
Certificate Holder Authorization	Domestic DV												
Certificate effective date	CVCA _{eff}												
Certificate expiration date	CVCA _{exp}												
Public Key reference	Public key of key pair DV_KEY_07a												

	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
--	-----------------------	--

2.4.7.6 DV_CERT_7d

ID	DV_CERT_7d															
Purpose	This certificate is a domestic DV certificate, which was issued by the update CVCA (LINK_CERT_7).															
Version	Smart-eID															
Referred by	Test case EAC2_ISO7816_M_3															
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 05 00 00 00 00 04 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>															
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTLINKDE007</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE007</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Domestic DV</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{exp} + 1 day</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{exp} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair AT_KEY_07</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_17</td> </tr> </table>		Certification Authority Reference	DETESTLINKDE007	Certificate Holder Reference	DETESTDVDE007	Certificate Holder Authorization	Domestic DV	Certificate effective date	CVCA _{exp} + 1 day	Certificate expiration date	CVCA _{exp} + 1 month	Public Key reference	Public key of key pair AT_KEY_07	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
Certification Authority Reference	DETESTLINKDE007															
Certificate Holder Reference	DETESTDVDE007															
Certificate Holder Authorization	Domestic DV															
Certificate effective date	CVCA _{exp} + 1 day															
Certificate expiration date	CVCA _{exp} + 1 month															
Public Key reference	Public key of key pair AT_KEY_07															
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17															

2.4.8 Certificate Set 8

This certificate set defines a link certificate used for the tests about the trust point update mechanism.

Note for ECDSA profile: Since the cryptographic mechanism is not changed by the link certificates defined in this certificate set, it must be stated by the vendor of the test sample if the domain parameters should be included. (see ICS A).

2.4.8.1 LINK_CERT_8

This link certificate is used to update the trust point defined by LINK_CERT_7.

ID	LINK_CERT_8																
Purpose	This certificate is a link certificate, based on the LINK_CERT_7																
Version	1.11																
Referred by	Test case EAC2_ISO7816_M_4																
Content definition	<p> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3 5F 25 06 gg 5F 24 06 hh <i>optional:</i> 65 vv ww 5F 37 ii jj </p> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>vv</i> is the encoded length of the certificate extension, <i>ww</i> is the placeholder for the certificate extension (vv bytes) </p>																
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>DETESTLINKDE007</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTLINKDE008</td></tr> <tr> <td>Certificate Holder Authorization</td><td>CVCA, DG 3, DG 4</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{exp} + 1 month</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{exp} + 4 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair CVCA_KEY_08</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_07</td></tr> <tr> <td>Certificate Extension</td><td>As defined by CVCA</td></tr> </table>	Certification Authority Reference	DETESTLINKDE007	Certificate Holder Reference	DETESTLINKDE008	Certificate Holder Authorization	CVCA, DG 3, DG 4	Certificate effective date	CVCA _{exp} + 1 month	Certificate expiration date	CVCA _{exp} + 4 month	Public Key reference	Public key of key pair CVCA_KEY_08	Signing Key reference	Signed with the private key of key pair CVCA_KEY_07	Certificate Extension	As defined by CVCA
Certification Authority Reference	DETESTLINKDE007																
Certificate Holder Reference	DETESTLINKDE008																
Certificate Holder Authorization	CVCA, DG 3, DG 4																
Certificate effective date	CVCA _{exp} + 1 month																
Certificate expiration date	CVCA _{exp} + 4 month																
Public Key reference	Public key of key pair CVCA_KEY_08																
Signing Key reference	Signed with the private key of key pair CVCA_KEY_07																
Certificate Extension	As defined by CVCA																

2.4.8.2 LINK_CERT_8a

This link certificate is used to update the trust point defined by LINK_CERT_7a

ID	LINK_CERT_8a	
Purpose	This certificate is a link certificate, based on the LINK_CERT_7a	
Version	Smart-eID	
Referred by	Test case EAC2 ISO7816 M 4	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 05 40 40 00 00 FF 5F 25 06 gg 5F 24 06 hh <i>optional:</i> 65 vv ww 5F 37 ii jj <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>vv</i> is the encoded length of the certificate extension, <i>ww</i> is the placeholder for the certificate extension (vv bytes)</p>	
Parameter	Certification Authority Reference DETESTLINKDE007 Certificate Holder Reference DETESTLINKDE008 Certificate Holder Authorization CVCA, all eID functions Certificate effective date CVCA _{exp} + 1 month Certificate expiration date CVCA _{exp} + 4 month Public Key reference Public key of key pair CVCA_KEY_08a Signing Key reference Signed with the private key of key pair CVCA_KEY_07 Certificate Extension As defined by CVCA	

2.4.9 Certificate Set 9

2.4.9.1 LINK_CERT_9

ID	LINK_CERT_9																	
Purpose	This certificate is a link certificate, based on the LINK_CERT_8																	
Version	1.11																	
Referred by	Test case EAC2 ISO7816 M 4																	
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3 5F 25 06 gg 5F 24 06 hh <i>optional:</i> 65 vv ww 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>vv</i> is the encoded length of the certificate extension, <i>ww</i> is the placeholder for the certificate extension (vv bytes)</p>																	
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTLINKDE008</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETEST_LINKDE009</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>CVCA, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{exp} + 3 month</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{exp} + 6 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair CVCA_KEY_09</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_08</td> </tr> <tr> <td>Certificate Extension</td> <td>As defined by CVCA</td> </tr> </table>		Certification Authority Reference	DETESTLINKDE008	Certificate Holder Reference	DETEST_LINKDE009	Certificate Holder Authorization	CVCA, DG 3, DG 4	Certificate effective date	CVCA _{exp} + 3 month	Certificate expiration date	CVCA _{exp} + 6 month	Public Key reference	Public key of key pair CVCA_KEY_09	Signing Key reference	Signed with the private key of key pair CVCA_KEY_08	Certificate Extension	As defined by CVCA
Certification Authority Reference	DETESTLINKDE008																	
Certificate Holder Reference	DETEST_LINKDE009																	
Certificate Holder Authorization	CVCA, DG 3, DG 4																	
Certificate effective date	CVCA _{exp} + 3 month																	
Certificate expiration date	CVCA _{exp} + 6 month																	
Public Key reference	Public key of key pair CVCA_KEY_09																	
Signing Key reference	Signed with the private key of key pair CVCA_KEY_08																	
Certificate Extension	As defined by CVCA																	

2.4.9.2 LINK_CERT_9a

ID	LINK_CERT_9a
Purpose	This certificate is a link certificate, based on the LINK_CERT_8a

Version	Smart-eID																
Referred by	Test case EAC2_ISO7816_M_4																
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 05 40 40 00 00 FF 5F 25 06 gg 5F 24 06 hh <i>optional:</i> 65 vv ww 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>vv</i> is the encoded length of the certificate extension, <i>ww</i> is the placeholder for the certificate extension (vv bytes)</p>																
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>DETESTLINKDE008</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETEST_LINKDE009</td></tr> <tr> <td>Certificate Holder Authorization</td><td>CVCA, all eID funktions</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{exp} + 3 month</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{exp} + 6 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair CVCA_KEY_09a</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_08</td></tr> <tr> <td>Certificate Extension</td><td>As defined by CVCA</td></tr> </table>	Certification Authority Reference	DETESTLINKDE008	Certificate Holder Reference	DETEST_LINKDE009	Certificate Holder Authorization	CVCA, all eID funktions	Certificate effective date	CVCA _{exp} + 3 month	Certificate expiration date	CVCA _{exp} + 6 month	Public Key reference	Public key of key pair CVCA_KEY_09a	Signing Key reference	Signed with the private key of key pair CVCA_KEY_08	Certificate Extension	As defined by CVCA
Certification Authority Reference	DETESTLINKDE008																
Certificate Holder Reference	DETEST_LINKDE009																
Certificate Holder Authorization	CVCA, all eID funktions																
Certificate effective date	CVCA _{exp} + 3 month																
Certificate expiration date	CVCA _{exp} + 6 month																
Public Key reference	Public key of key pair CVCA_KEY_09a																
Signing Key reference	Signed with the private key of key pair CVCA_KEY_08																
Certificate Extension	As defined by CVCA																

2.4.9.3 DV_CERT_9

ID	DV_CERT_9
Purpose	This certificate is a domestic DV certificate, which was issued by LINK_CERT_9.
Version	1.11
Referred by	Test case EAC2_ISO7816_M_4
Content definition	7F 21 aa

	<pre> 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>
Parameter	Certification Authority Reference
	DETEST_LINKDE009
	Certificate Holder Reference
	DETESTDVDE009
	Certificate Holder Authorization
	domestic DV, DG 3, DG 4
	Certificate effective date

2.4.9.4 DV_CERT_9a

ID	DV_CERT_9a
Purpose	This certificate is a domestic DV certificate, which was issued by LINK_CERT_9a.
Version	1.11
Referred by	Test case EAC2_ISO7816_M_4
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 05 40 40 00 00 FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects </p>

	<p><i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	DETEST_LINKDE009
	Certificate Holder Reference	DETESTDVDE009
	Certificate Holder Authorization	domestic DV, all eID functions
	Certificate effective date	CVCA _{exp} + 3 month
	Certificate expiration date	CVCA _{exp} + 4 month
	Public Key reference	Public key of key pair DV_KEY_09a
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_09

2.4.10 Certificate Set 10

2.4.10.1 LINK_CERT_10

ID	LINK_CERT_10
Purpose	This certificate is an irregular IS CVCA certificate. The signing key is a DV key.
Version	1.11
Referred by	Test case EAC2_ISO7816_J_41, Test case EAC2_ISO7816_J_42
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3 5F 25 06 gg 5F 24 06 hh optional: 65 vv ww 5F 37 ii jj </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference</p>

	yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes) vv is the encoded length of the certificate extension, ww is the placeholder for the certificate extension (vv bytes)	
Parameter	Certification Authority Reference	DETESTDVDE010
	Certificate Holder Reference	As defined by the initial CVCA root
	Certificate Holder Authorization	CVCA, DG 3, DG 4
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{exp}
	Public Key reference	Public key of key pair CVCA_KEY_00
	Signing Key reference	Signed with the private key of key pair DV_KEY_10
	Certificate Extension	As defined by CVCA

2.4.10.2 DV_CERT_10a

ID	DV_CERT_10a	
Purpose	This certificate is a regular domestic DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.	
Version	1.11	
Referred by	Test case EAC2_ISO7816_J_41, Test case EAC2_ISO7816_J_43, Test case EAC2_ISO7816_J_44	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj <p>aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	As defined by the CVCA

Certificate Holder Reference	DETTESTDVDE010
Certificate Holder Authorization	domestic DV, DG 3, DG 4
Certificate effective date	CVCA _{eff}
Certificate expiration date	CVCA _{eff} + 1 month
Public Key reference	Public key of key pair DV_KEY_10
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.10.3 DV_CERT_10b

ID	DV_CERT_10b														
Purpose	This certificate is a regular foreign DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.														
Version	1.11														
Referred by	Test case EAC2_ISO7816_J_42, Test case EAC2_ISO7816_J_45, Test case EAC2_ISO7816_J_46														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 43 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p>aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETTESTDVDE010</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>foreign DV, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_10</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_00</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETTESTDVDE010	Certificate Holder Authorization	foreign DV, DG 3, DG 4	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_10	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETTESTDVDE010														
Certificate Holder Authorization	foreign DV, DG 3, DG 4														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_10														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.10.4 DV_CERT_10c

ID	DV_CERT_10c														
Purpose	This certificate is an irregular DV domestic certificate. The signing key is a DV key.														
Version	1.11														
Referred by	Test case EAC2 ISO7816 J 43, Test case EAC2 ISO7816 J 45														
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>DETESTDVDE010</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTDVDE110</td></tr> <tr> <td>Certificate Holder Authorization</td><td>domestic DV, DG 3, DG 4</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 1 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair DV_KEY_10</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair DV_KEY_10</td></tr> </table>	Certification Authority Reference	DETESTDVDE010	Certificate Holder Reference	DETESTDVDE110	Certificate Holder Authorization	domestic DV, DG 3, DG 4	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_10	Signing Key reference	Signed with the private key of key pair DV_KEY_10
Certification Authority Reference	DETESTDVDE010														
Certificate Holder Reference	DETESTDVDE110														
Certificate Holder Authorization	domestic DV, DG 3, DG 4														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_10														
Signing Key reference	Signed with the private key of key pair DV_KEY_10														

2.4.10.5 DV_CERT_10d

ID	DV_CERT_10d
Purpose	This certificate is an irregular DV foreign certificate. The signing key is a DV key.
Version	1.11
Referred by	Test case EAC2 ISO7816 J 44, Test case EAC2 ISO7816 J 46
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff </pre>

	<pre> 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 43 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>														
Parameter	<table border="1"> <tr><td>Certification Authority Reference</td><td>DETESTDVDE010</td></tr> <tr><td>Certificate Holder Reference</td><td>DETESTDVDE110</td></tr> <tr><td>Certificate Holder Authorization</td><td>foreign DV, DG 3, DG 4</td></tr> <tr><td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr><td>Certificate expiration date</td><td>CVCA_{eff} + 1 month</td></tr> <tr><td>Public Key reference</td><td>Public key of key pair DV_KEY_10</td></tr> <tr><td>Signing Key reference</td><td>Signed with the private key of key pair DV_KEY_10</td></tr> </table>	Certification Authority Reference	DETESTDVDE010	Certificate Holder Reference	DETESTDVDE110	Certificate Holder Authorization	foreign DV, DG 3, DG 4	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_10	Signing Key reference	Signed with the private key of key pair DV_KEY_10
Certification Authority Reference	DETESTDVDE010														
Certificate Holder Reference	DETESTDVDE110														
Certificate Holder Authorization	foreign DV, DG 3, DG 4														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_10														
Signing Key reference	Signed with the private key of key pair DV_KEY_10														

2.4.10.6 IS_CERT_10

ID	IS_CERT_10
Purpose	This certificate is an irregular domestic IS certificate. This IS certificate is signed by the CVCA key.
Version	1.11
Referred by	Test case EAC2_ISO7816_J_40
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, </p>

	ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)	
Parameter	Certification Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTISDE010
	Certificate Holder Authorization	IS, DG 3, DG 4
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 13 days
	Public Key reference	Public key of key pair IS_KEY_10
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.11 Certificate Set 11

2.4.11.1 LINK_CERT_11a

ID	LINK_CERT_11a
Purpose	This certificate is an irregular IS CVCA certificate. The signing key is an IS key.
Version	1.11
Referred by	Test case EAC2 ISO7816 J 50
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3 5F 25 06 gg 5F 24 06 hh 65 vv ww 5F 37 ii jj </pre> <p> aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes) </p>

	<i>vv</i> is the encoded length of the certificate extension, <i>ww</i> is the placeholder for the certificate extension (<i>vv</i> bytes)	
Parameter	Certification Authority Reference	DETESTISDE011
	Certificate Holder Reference	As defined by the initial CVCA root
	Certificate Holder Authorization	CVCA, DG 3, DG 4
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{exp}
	Public Key reference	Public key of key pair CVCA_KEY_00
	Signing Key reference	Signed with the private key of key pair IS_KEY_11
	Certificate Extension	As defined by CVCA

2.4.11.2 LINK_CERT_11b

ID	LINK_CERT_11b									
Purpose	This certificate is a valid link certificate.									
Version	1.11									
Referred by	Test case EAC2_ISO7816_M_5									
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3 5F 25 06 gg 5F 24 06 hh <i>optional:</i> 65 vv ww 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (<i>cc</i> bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (<i>ee</i> bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (<i>xx</i> bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (<i>ii</i> bytes) <i>vv</i> is the encoded length of the certificate extension, <i>ww</i> is the placeholder for the certificate extension (<i>vv</i> bytes)</p>									
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETEST_LINKDE009</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETEST_LINKDE011</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>CVCA, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{exp} + 5 months</td> </tr> </table>		Certification Authority Reference	DETEST_LINKDE009	Certificate Holder Reference	DETEST_LINKDE011	Certificate Holder Authorization	CVCA, DG 3, DG 4	Certificate effective date	CVCA _{exp} + 5 months
Certification Authority Reference	DETEST_LINKDE009									
Certificate Holder Reference	DETEST_LINKDE011									
Certificate Holder Authorization	CVCA, DG 3, DG 4									
Certificate effective date	CVCA _{exp} + 5 months									

Certificate expiration date	CVCA _{exp} + 8 months
Public Key reference	Public key of key pair CVCA_KEY_11
Signing Key reference	Signed with the private key of key pair CVCA_KEY_09
Certificate Extension	As defined by CVCA

2.4.11.3 LINK_CERT_11c

ID	LINK CERT 11c																
Purpose	This certificate is a valid link certificate.																
Version	Smart-eID																
Referred by	Test case EAC2 ISO7816 M 5																
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 05 40 40 00 00 FF 5F 25 06 gg 5F 24 06 hh optional: 65 vv ww 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>vv</i> is the encoded length of the certificate extension, <i>ww</i> is the placeholder for the certificate extension (vv bytes)</p>																
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETEST_LINKDE009</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETEST_LINKDE011</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>CVCA, all eID functions</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{exp} + 5 months</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{exp} + 8 months</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair CVCA_KEY_11a</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_09</td> </tr> <tr> <td>Certificate Extension</td> <td>As defined by CVCA</td> </tr> </table>	Certification Authority Reference	DETEST_LINKDE009	Certificate Holder Reference	DETEST_LINKDE011	Certificate Holder Authorization	CVCA, all eID functions	Certificate effective date	CVCA _{exp} + 5 months	Certificate expiration date	CVCA _{exp} + 8 months	Public Key reference	Public key of key pair CVCA_KEY_11a	Signing Key reference	Signed with the private key of key pair CVCA_KEY_09	Certificate Extension	As defined by CVCA
Certification Authority Reference	DETEST_LINKDE009																
Certificate Holder Reference	DETEST_LINKDE011																
Certificate Holder Authorization	CVCA, all eID functions																
Certificate effective date	CVCA _{exp} + 5 months																
Certificate expiration date	CVCA _{exp} + 8 months																
Public Key reference	Public key of key pair CVCA_KEY_11a																
Signing Key reference	Signed with the private key of key pair CVCA_KEY_09																
Certificate Extension	As defined by CVCA																

2.4.11.4 DV_CERT_11a

ID	DV_CERT_11a														
Purpose	This certificate is a regular domestic DV certificate, which validity period starts at the effective date of the CVCA and expires after one month.														
Version	1.11														
Referred by	Test case EAC2_ISO7816_J_47, Test case EAC2_ISO7816_J_48, Test case EAC2_ISO7816_J_49, Test case EAC2_ISO7816_J_50														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE011</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>domestic DV, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_11</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_00</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE011	Certificate Holder Authorization	domestic DV, DG 3, DG 4	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_11	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETESTDVDE011														
Certificate Holder Authorization	domestic DV, DG 3, DG 4														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_11														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.11.5 DV_CERT_11b

ID	DV_CERT_11b
Purpose	This certificate is an irregular foreign DV certificate. The signing key is an IS key.
Version	1.11
Referred by	Test case EAC2_ISO7816_J_47
Content	7F 21 aa

definition	<pre> 7F 4E <i>bb</i> 5F 29 01 00 42 <i>cc dd</i> 7F 49 <i>ee ff</i> 5F 20 <i>xx yy</i> 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 43 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> 5F 37 <i>ii jj</i> </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>
Parameter	Certification Authority Reference
	DETESTISDE011
	Certificate Holder Reference
	DETESTDVDE011
	Certificate Holder Authorization
	foreign DV, DG 3, DG 4
	Public Key reference

2.4.11.6 DV_CERT_11c

ID	DV_CERT_11c
Purpose	This certificate is an irregular domestic DV certificate. The signing key is an IS key.
Version	1.11
Referred by	Test case EAC2 ISO7816 J 48
Content definition	<pre> 7F 21 <i>aa</i> 7F 4E <i>bb</i> 5F 29 01 00 42 <i>cc dd</i> 7F 49 <i>ee ff</i> 5F 20 <i>xx yy</i> 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> 5F 37 <i>ii jj</i> </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object</p>

	<p><i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	DETESTISDE011
	Certificate Holder Reference	DETESTDVDE011
	Certificate Holder Authorization	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_11
	Signing Key reference	Signed with the private key of key pair IS_KEY_11

2.4.11.7 DV_CERT_11d

ID	DV_CERT_11d	
Purpose	This certificate is a regular domestic DV certificate, which validity period starts at the effective date of the referencing CVCA 11b and expires after one month.	
Version	EAC2_1.0	
Referred by	Test case EAC2_ISO7816_M_8	
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	DETEST_LINKDE011

Certificate Holder Reference	DETESTDVDE011
Certificate Holder Authorization	domestic DV, DG 3, DG 4
Certificate effective date	CVCA _{exp} + 5 months
Certificate expiration date	CVCA _{exp} + 6 months
Public Key reference	Public key of key pair DV_KEY_11
Signing Key reference	Signed with the private key of key pair CVCA_KEY_11

2.4.11.8 IS_CERT_11a

ID	IS_CERT_11a														
Purpose	This certificate is a regular IS certificate.														
Version	1.11														
Referred by	Test case EAC2_ISO7816_J_47, Test case EAC2_ISO7816_J_48, Test case EAC2_ISO7816_J_49, Test case EAC2_ISO7816_J_50														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p>aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTDVDE011</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTISDE011</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>IS, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 13 days</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair IS_KEY_11</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair DV_KEY_11</td> </tr> </table>	Certification Authority Reference	DETESTDVDE011	Certificate Holder Reference	DETESTISDE011	Certificate Holder Authorization	IS, DG 3, DG 4	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 13 days	Public Key reference	Public key of key pair IS_KEY_11	Signing Key reference	Signed with the private key of key pair DV_KEY_11
Certification Authority Reference	DETESTDVDE011														
Certificate Holder Reference	DETESTISDE011														
Certificate Holder Authorization	IS, DG 3, DG 4														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 13 days														
Public Key reference	Public key of key pair IS_KEY_11														
Signing Key reference	Signed with the private key of key pair DV_KEY_11														

2.4.11.9 IS_CERT_11b

ID	IS_CERT_11b														
Purpose	This certificate is an irregular IS certificate. The signing key is an IS key.														
Version	1.11														
Referred by	Test case EAC2 ISO7816 J 49														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTISDE011</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTISDE111</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>IS, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 13 days</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair IS_KEY_11</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair IS_KEY_11</td> </tr> </table>	Certification Authority Reference	DETESTISDE011	Certificate Holder Reference	DETESTISDE111	Certificate Holder Authorization	IS, DG 3, DG 4	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 13 days	Public Key reference	Public key of key pair IS_KEY_11	Signing Key reference	Signed with the private key of key pair IS_KEY_11
Certification Authority Reference	DETESTISDE011														
Certificate Holder Reference	DETESTISDE111														
Certificate Holder Authorization	IS, DG 3, DG 4														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 13 days														
Public Key reference	Public key of key pair IS_KEY_11														
Signing Key reference	Signed with the private key of key pair IS_KEY_11														

2.4.11.10 IS_CERT_11c

ID	IS_CERT_11c
Purpose	This certificate is an irregular IS certificate. The signing key is a CVCA key.
Version	1.11
Referred by	Test case EAC2 ISO7816 M 5
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff</p>

	<pre> 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>
Parameter	Certification Authority Reference
	DETEST_LINKDE011
	Certificate Holder Reference
	DETESTISDE011
	Certificate Holder Authorization
	IS, DG 3, DG 4
	Certificate effective date

2.4.11.11 AT_CERT_11a

ID	AT_CERT_11a
Purpose	This certificate is an irregular AT certificate. The signing key is a CVCA key.
Version	Smart-eID
Referred by	Test case EAC2 ISO7816 M 5
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 05 00 00 00 00 04 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, </p>

	ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)	
Parameter	Certification Authority Reference	DETEST_LINKDE011
	Certificate Holder Reference	DETESTATDE011
	Certificate Holder Authorization	Authentication Terminal
	Certificate effective date	CVCA _{exp} + 5 months
	Certificate expiration date	CVCA _{exp} + 6 months
	Public Key reference	Public key of key pair AT_KEY_11
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_11

2.4.12 Certificate Set 12

This certificate set is used for the certificate structure tests.

2.4.12.1 DV_CERT_12a

ID	DV_CERT_12a
Purpose	This certificate is a domestic DV certificate.
Version	1.11
Referred by	Test case EAC2_ISO7816_J_23, Test case EAC2_ISO7816_J_33
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj <p>aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate</p>

	<i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (<i>ii</i> bytes)	
Parameter	Certification Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETTESTDVDE012
	Certificate Holder Authorization	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA _{eff} + 1 month + 20 days
	Certificate expiration date	CVCA _{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.12.2 DV_CERT_12b

ID	DV_CERT_12b	
Purpose	Certificate with a wrong “certificate body” tag	
Version	1.11	
Referred by	Test case EAC2_ISO7816_J_24	
Content definition	7F 21 aa 7F 4F bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (<i>cc</i> bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (<i>ee</i> bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (<i>xx</i> bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (<i>ii</i> bytes)</p>	
Parameter	Certification Authority Reference Certificate Holder Reference Certificate Holder Authorization Certificate effective date Certificate expiration date Public Key reference	
	As defined by the CVCA DETTESTDVDE012 domestic DV, DG 3, DG 4 CVCA _{eff} + 1 month + 20 days CVCA _{eff} + 1 month + 25 days Public key of key pair DV KEY_12	

	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
--	-----------------------	--

2.4.12.3 DV_CERT_12c

ID	DV_CERT_12c															
Purpose	Certificate with a wrong “certificate signature” tag															
Version	1.11															
Referred by	Test case EAC2 ISO7816 J 25															
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 38 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>															
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE012</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>domestic DV, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff} + 1 month + 20 days</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month + 25 days</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_12</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_00</td> </tr> </table>		Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE012	Certificate Holder Authorization	domestic DV, DG 3, DG 4	Certificate effective date	CVCA _{eff} + 1 month + 20 days	Certificate expiration date	CVCA _{eff} + 1 month + 25 days	Public Key reference	Public key of key pair DV_KEY_12	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA															
Certificate Holder Reference	DETESTDVDE012															
Certificate Holder Authorization	domestic DV, DG 3, DG 4															
Certificate effective date	CVCA _{eff} + 1 month + 20 days															
Certificate expiration date	CVCA _{eff} + 1 month + 25 days															
Public Key reference	Public key of key pair DV_KEY_12															
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00															

2.4.12.4 DV_CERT_12d

ID	DV_CERT_12d
Purpose	Certificate with an inconsistent “certificate body” DO (wrong length)
Version	1.11
Referred by	Test case EAC2 ISO7816 J 26
Content	7F 21 aa

definition	<pre> 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object decreased by one <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>
Parameter	Certification Authority Reference
	As defined by the CVCA
	Certificate Holder Reference
	DETESTDVDE012
	Certificate Holder Authorization
	domestic DV, DG 3, DG 4
	Certificate effective date

2.4.12.5 DV_CERT_12e

ID	DV_CERT_12e
Purpose	Certificate with an inconsistent “certificate signature” DO (The length byte specifies one byte less than the actual signature length)
Version	1.11
Referred by	Test case EAC2_ISO7816_J_27
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre>

	<p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object decreased by one, <i>jj</i> is the placeholder for the certificates signature (<i>ii</i> + 1 bytes)</p>	
Parameter	Certification Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorization	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA _{eff} + 1 month + 20 days
	Certificate expiration date	CVCA _{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.12.6 DV_CERT_12f

ID	DV_CERT_12f
Purpose	Certificate with a wrong signature
Version	1.11
Referred by	Test case EAC2 ISO7816 J 28
Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object,</p>

	<i>jj</i> is the placeholder for the certificates signature (ii bytes) last byte is increased by one (mod 256)	
Parameter	Certification Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETTESTDVDE012
	Certificate Holder Authorization	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA _{eff} + 1 month + 20 days
	Certificate expiration date	CVCA _{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.12.7 DV_CERT_12g

ID	DV_CERT_12g												
Purpose	Certificate with a wrong signature												
Version	1.11												
Referred by	Test case EAC2_ISO7816_J_29												
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) – last byte is dropped and ii is updated according to the new length </p>												
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETTESTDVDE012</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>domestic DV, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff} + 1 month + 20 days</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month + 25 days</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV KEY_12</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETTESTDVDE012	Certificate Holder Authorization	domestic DV, DG 3, DG 4	Certificate effective date	CVCA _{eff} + 1 month + 20 days	Certificate expiration date	CVCA _{eff} + 1 month + 25 days	Public Key reference	Public key of key pair DV KEY_12
Certification Authority Reference	As defined by the CVCA												
Certificate Holder Reference	DETTESTDVDE012												
Certificate Holder Authorization	domestic DV, DG 3, DG 4												
Certificate effective date	CVCA _{eff} + 1 month + 20 days												
Certificate expiration date	CVCA _{eff} + 1 month + 25 days												
Public Key reference	Public key of key pair DV KEY_12												

	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
--	-----------------------	---

2.4.12.8 DV_CERT_12h

ID	DV_CERT_12h															
Purpose	Modification in the certificate public key: OID is missing															
Version	1.11															
Referred by	Test case EAC2 ISO7816 J 35															
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes) – it does not contain any OID DO, <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>															
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE012</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>domestic DV, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff} + 1 month + 20 days</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month + 25 days</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_12</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_00</td> </tr> </table>		Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE012	Certificate Holder Authorization	domestic DV, DG 3, DG 4	Certificate effective date	CVCA _{eff} + 1 month + 20 days	Certificate expiration date	CVCA _{eff} + 1 month + 25 days	Public Key reference	Public key of key pair DV_KEY_12	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA															
Certificate Holder Reference	DETESTDVDE012															
Certificate Holder Authorization	domestic DV, DG 3, DG 4															
Certificate effective date	CVCA _{eff} + 1 month + 20 days															
Certificate expiration date	CVCA _{eff} + 1 month + 25 days															
Public Key reference	Public key of key pair DV_KEY_12															
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00															

2.4.12.9 DV_CERT_12i

ID	DV_CERT_12i
Purpose	Modification in the certificate public key: wrong OID
Version	1.11
Referred by	Test case EAC2 ISO7816 J 34

Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes) – the OID has an incorrect value that does not indicate id-TA: (0.4.0.127.0.7.2.2.3.x.y), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>
Parameter	Certification Authority Reference
	As defined by the CVCA
	Certificate Holder Reference
	DETESTDVDE012
	Certificate Holder Authorization
	domestic DV, DG 3, DG 4
	Certificate effective date

2.4.12.10 DV_CERT_12j

ID	DV_CERT_12j
Purpose	For ECDSA profile only: Modification in the certificate public key: the elliptic curve public point is missing
Version	1.11
Referred by	Test case EAC2 ISO7816 J 36
Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh</pre>

	5F 37 ii jj aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes) – The elliptic curve public point is missing, xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)
Parameter	Certification Authority Reference
	As defined by the CVCA
	Certificate Holder Reference
	DETESTDVDE012
	Certificate Holder Authorization
	domestic DV, DG 3, DG 4
	Certificate effective date

2.4.12.11 DV_CERT_12k

ID	DV_CERT_12k
Purpose	For RSA profile only: Modification in the certificate public key: the RSA modulus is missing
Version	1.11
Referred by	Test case EAC2_ISO7816_J_37
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes) – The RSA modulus is missing.

	xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)	
Parameter	Certification Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012
	Certificate Holder Authorization	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA _{eff} + 1 month + 20 days
	Certificate expiration date	CVCA _{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.12.12 DV_CERT_12I

ID	DV CERT 12I	
Purpose	For RSA profile only: Modification in the certificate public key: the RSA public exponent is missing	
Version	1.11	
Referred by	Test case EAC2 ISO7816 J 38	
Content definition	$7F\ 21\ aa$ $7F\ 4E\ bb$ $5F\ 29\ 01\ 00$ $42\ cc\ dd$ $7F\ 49\ ee\ ff$ $5F\ 20\ xx\ yy$ $7F\ 4C\ 0E\ 06\ 09\ 04\ 00\ 7F\ 00\ 07\ 03\ 01\ 02\ 01\ 53\ 01\ 83$ $5F\ 25\ 06\ gg$ $5F\ 24\ 06\ hh$ $5F\ 37\ ii\ jj$ <p>aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes) – The RSA public exponent is missing, xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE012

Certificate Holder Authorization	domestic DV, DG 3, DG 4
Certificate effective date	CVCA _{eff} + 1 month + 20 days
Certificate expiration date	CVCA _{eff} + 1 month + 25 days
Public Key reference	Public key of key pair DV_KEY_12
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.12.13 DV_CERT_12m

ID	DV CERT 12m														
Purpose	Modification in the certificate public key: For ECDSA profile: an unknown DO is present within the EC parameters (tag '77'), For RSA profile: an unknown DO is present within the RSA parameters ('77 01 00')														
Version	1.11														
Referred by	Test case EAC2 ISO7816 J 39														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes) – An unknown DO '77 is present <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE012</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>domestic DV, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}+ 1 month + 20 days</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff}+ 1 month + 25 days</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_12</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_00</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE012	Certificate Holder Authorization	domestic DV, DG 3, DG 4	Certificate effective date	CVCA _{eff} + 1 month + 20 days	Certificate expiration date	CVCA _{eff} + 1 month + 25 days	Public Key reference	Public key of key pair DV_KEY_12	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETESTDVDE012														
Certificate Holder Authorization	domestic DV, DG 3, DG 4														
Certificate effective date	CVCA _{eff} + 1 month + 20 days														
Certificate expiration date	CVCA _{eff} + 1 month + 25 days														
Public Key reference	Public key of key pair DV_KEY_12														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.12.14 DV_CERT_12n

ID	DV_CERT_12n
Version	Has been merged with DV_CERT_12m in version 1.1

2.4.12.15 DV_CERT_12o

ID	DV_CERT_12o														
Purpose	For RSA profile only: Certificate with a wrong signature														
Version	1.11														
Referred by	Test case EAC2 ISO7816 J 30														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) – the signature is greater than the modulus of the issuing key CVCA_KEY_00, the length of signature matches the length of the modulus</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE012</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>domestic DV, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff} + 1 month + 20 days</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month + 25 days</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_12</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_00</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE012	Certificate Holder Authorization	domestic DV, DG 3, DG 4	Certificate effective date	CVCA _{eff} + 1 month + 20 days	Certificate expiration date	CVCA _{eff} + 1 month + 25 days	Public Key reference	Public key of key pair DV_KEY_12	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETESTDVDE012														
Certificate Holder Authorization	domestic DV, DG 3, DG 4														
Certificate effective date	CVCA _{eff} + 1 month + 20 days														
Certificate expiration date	CVCA _{eff} + 1 month + 25 days														
Public Key reference	Public key of key pair DV_KEY_12														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.12.16 DV_CERT_12p

ID	DV_CERT_12p
----	-------------

Purpose	For ECDSA profile only: The certificate signature is wrong. It is obtained by filling the ‘r’ part of the signature with ‘00’. The length of ‘r’ is still matches the size of the prime.														
Version	1.11														
Referred by	Test case EAC2 ISO7816 J 31														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) – with r = 0</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>As defined by the CVCA</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTDVDE012</td></tr> <tr> <td>Certificate Holder Authorization</td><td>domestic DV, DG 3, DG 4</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff} + 1 month + 20 days</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 1 month + 25 days</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair DV_KEY_12</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_00</td></tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE012	Certificate Holder Authorization	domestic DV, DG 3, DG 4	Certificate effective date	CVCA _{eff} + 1 month + 20 days	Certificate expiration date	CVCA _{eff} + 1 month + 25 days	Public Key reference	Public key of key pair DV_KEY_12	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETESTDVDE012														
Certificate Holder Authorization	domestic DV, DG 3, DG 4														
Certificate effective date	CVCA _{eff} + 1 month + 20 days														
Certificate expiration date	CVCA _{eff} + 1 month + 25 days														
Public Key reference	Public key of key pair DV_KEY_12														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.12.17 DV_CERT_12q

ID	DV_CERT_12q
Purpose	For ECDSA profile only: The certificate signature is wrong. It is obtained by filling the ‘s’ part of the signature with ‘00’. The length of ‘s’ is still matches the size of the prime.
Version	1.11
Referred by	Test case EAC2 ISO7816 J 32
Content definition	7F 21 aa 7F 4E bb

	<pre> 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre>	
<p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) – with s = 0</p>		
Parameter	Certification Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETTESTDVDE012
	Certificate Holder Authorization	domestic DV, DG 3, DG 4
	Certificate effective date	CVCA _{eff} + 1 month + 20 days
	Certificate expiration date	CVCA _{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_12
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00

2.4.13 Certificate Set 13

This certificate set defines a link certificate used to update the chip signature mechanism according to the migration policy as defined by the manufacturer. The cryptographic elements of these certificates MUST use the new mechanisms besides the signature of the LINK_CERT_13 which is done with the original signature mechanism. This certificate set is only needed if the “Migration” profile is supported.

2.4.13.1 LINK_CERT_13a

Note for ECDSA profile: Since the cryptographic mechanism is changed by this certificate, the domain parameters MUST be included in this certificate.

ID	LINK CERT_13a
Purpose	For MIG profile only: This certificate is a link certificate, which defines a new cryptographic mechanism to be used by chip.
Version	1.11
Referred by	Test case EAC2_ISO7816_N_1
Content	7F 21 aa

definition	<pre> 7F 4E <i>bb</i> 5F 29 01 00 42 <i>cc dd</i> 7F 49 <i>ee ff</i> 5F 20 <i>xx yy</i> 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> <i>optional</i> 65 <i>vv ww</i> 5F 37 <i>ii jj</i> </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>vv</i> is the encoded length of the certificate extension, <i>ww</i> is the placeholder for the certificate extension (vv bytes) </p>																
Parameter	<table border="1"> <tr><td>Certification Authority Reference</td><td>DETEST_LINKDE011</td></tr> <tr><td>Certificate Holder Reference</td><td>DETESTLINKDE013</td></tr> <tr><td>Certificate Holder Authorization</td><td>CVCA, DG 3, DG 4</td></tr> <tr><td>Certificate effective date</td><td>CVCA_{exp} + 7 months</td></tr> <tr><td>Certificate expiration date</td><td>CVCA_{exp} + 10 month</td></tr> <tr><td>Public Key reference</td><td>Public key of key pair CVCA_KEY_13</td></tr> <tr><td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_11</td></tr> <tr><td>Certificate Extension</td><td>As defined by CVCA</td></tr> </table>	Certification Authority Reference	DETEST_LINKDE011	Certificate Holder Reference	DETESTLINKDE013	Certificate Holder Authorization	CVCA, DG 3, DG 4	Certificate effective date	CVCA _{exp} + 7 months	Certificate expiration date	CVCA _{exp} + 10 month	Public Key reference	Public key of key pair CVCA_KEY_13	Signing Key reference	Signed with the private key of key pair CVCA_KEY_11	Certificate Extension	As defined by CVCA
Certification Authority Reference	DETEST_LINKDE011																
Certificate Holder Reference	DETESTLINKDE013																
Certificate Holder Authorization	CVCA, DG 3, DG 4																
Certificate effective date	CVCA _{exp} + 7 months																
Certificate expiration date	CVCA _{exp} + 10 month																
Public Key reference	Public key of key pair CVCA_KEY_13																
Signing Key reference	Signed with the private key of key pair CVCA_KEY_11																
Certificate Extension	As defined by CVCA																

2.4.13.2 DV_CERT_13a

ID	DV_CERT_13a
Purpose	For MIG profile only: This certificate is a domestic DV certificate, which was issued by the new CVCA.
Version	1.11
Referred by	Test case EAC2_ISO7816_N_1
Content definition	7F 21 <i>aa</i> 7F 4E <i>bb</i> 5F 29 01 00

	<pre> 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <code>aa</code> is the encoded combined length of certificate body and signature objects <code>bb</code> is the encoded length of the certificate body object <code>cc</code> is the encoded length of the Certification Authority Reference <code>dd</code> is the placeholder for the Certification Authority Reference (cc bytes) <code>ee</code> is the encoded length of the certificate's public key, <code>ff</code> is the placeholder for the certificate's public key bytes (ee bytes), <code>xx</code> is the encoded length of the Certificate Holder Reference <code>yy</code> is the placeholder for the Certificate Holder Reference (xx bytes) <code>gg</code> is the placeholder for the BCD encoded effective date of the certificate <code>hh</code> is the placeholder for the BCD encoded expiration date of the certificate <code>ii</code> is the encoded length of the certificates signature object, <code>jj</code> is the placeholder for the certificates signature (ii bytes) </p>
Parameter	Certification Authority Reference
	DETEST_LINKDE013
	Certificate Holder Reference
	DETESTDVDE013
	Certificate Holder Authorization
	domestic DV, DG 3, DG 4
	Certificate effective date

2.4.13.3 IS_CERT_13a

ID	IS_CERT_13a
Purpose	For MIG profile only: This certificate is a regular IS certificate, which is issued by the DV_CERT_13a.
Version	1.11
Referred by	Test case EAC2 ISO7816_N_1
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <code>aa</code> is the encoded combined length of certificate body and signature objects <code>bb</code> is the encoded length of the certificate body object <code>cc</code> is the encoded length of the Certification Authority Reference <code>dd</code> is the placeholder for the Certification Authority Reference (cc bytes) </p>

	<p><i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (<i>ee</i> bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (<i>xx</i> bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (<i>ii</i> bytes)</p>	
Parameter	Certification Authority Reference	DETESTDVDE013
	Certificate Holder Reference	DETESTISDE013
	Certificate Holder Authorization	IS, DG 3, DG 4
	Certificate effective date	CVCA _{exp} + 7 months
	Certificate expiration date	CVCA _{exp} + 8 months
	Public Key reference	Public key of key pair IS_KEY_13
	Signing Key reference	Signed with the private key of key pair DV_KEY_13

2.4.13.4 LINK_CERT_13b

Note for ECDSA profile: Since the cryptographic mechanism is changed by this certificate, the domain parameters MUST be included in this certificate.

ID	LINK_CERT_13b
Purpose	For MIG profile only: This certificate is a link certificate, which defines a new cryptographic mechanism to be used by chip.
Version	1.2
Referred by	Test case EAC2 ISO7816_N2
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 C3 5F 25 06 gg 5F 24 06 hh optional 65 vv ww 5F 37 ii jj </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (<i>cc</i> bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (<i>ee</i> bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (<i>xx</i> bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object,</p>

	<i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>vv</i> is the encoded length of the certificate extension, <i>ww</i> is the placeholder for the certificate extension (vv bytes)	
Parameter	Certification Authority Reference	DETEST_LINKDE011
	Certificate Holder Reference	DETESTLINKDE013
	Certificate Holder Authorization	CVCA, DG 3, DG 4
	Certificate effective date	CVCA _{exp} + 7 months
	Certificate expiration date	CVCA _{exp} + 10 month
	Public Key reference	Public key of key pair CVCA_KEY_13
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_11
	Certificate Extension	As defined by CVCA

2.4.13.5 DV_CERT_13b

ID	DV_CERT_13b								
Purpose	For MIG profile only: This certificate is a domestic DV certificate, which was issued by the new CVCA.								
Version	1.2								
Referred by	Test case EAC2_ISO7816_N2								
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>								
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETEST_LINKDE013</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE013</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>domestic DV, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{exp} + 7 months</td> </tr> </table>	Certification Authority Reference	DETEST_LINKDE013	Certificate Holder Reference	DETESTDVDE013	Certificate Holder Authorization	domestic DV, DG 3, DG 4	Certificate effective date	CVCA _{exp} + 7 months
Certification Authority Reference	DETEST_LINKDE013								
Certificate Holder Reference	DETESTDVDE013								
Certificate Holder Authorization	domestic DV, DG 3, DG 4								
Certificate effective date	CVCA _{exp} + 7 months								

	Certificate expiration date	CVCA _{exp} + 8 months
	Public Key reference	Public key of key pair DV_KEY_13
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_13

2.4.13.6 AT_CERT_13b

ID	AT_CERT_13b															
Purpose	For MIG profile only: This certificate is a regular IS certificate, which is issued by the DV_CERT_13b.															
Version	1.2															
Referred by	Test case EAC2 ISO7816 N2															
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>															
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTDVDE013</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTATDE013</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>IS, DG 3, DG 4</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{exp} + 7 months</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{exp} + 8 months</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair IS_KEY_13</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair DV_KEY_13</td> </tr> </table>		Certification Authority Reference	DETESTDVDE013	Certificate Holder Reference	DETESTATDE013	Certificate Holder Authorization	IS, DG 3, DG 4	Certificate effective date	CVCA _{exp} + 7 months	Certificate expiration date	CVCA _{exp} + 8 months	Public Key reference	Public key of key pair IS_KEY_13	Signing Key reference	Signed with the private key of key pair DV_KEY_13
Certification Authority Reference	DETESTDVDE013															
Certificate Holder Reference	DETESTATDE013															
Certificate Holder Authorization	IS, DG 3, DG 4															
Certificate effective date	CVCA _{exp} + 7 months															
Certificate expiration date	CVCA _{exp} + 8 months															
Public Key reference	Public key of key pair IS_KEY_13															
Signing Key reference	Signed with the private key of key pair DV_KEY_13															

2.4.14 Certificate Set 14

The certificate set follows a certification scheme where the DV and IS contain public key information from a generated key whose lengths are shorter than the CVCA key length.

2.4.14.1 DV_CERT_14a

ID	DV_CERT_14a														
Purpose	This certificate is a regular domestic DV certificate which is issued by the CVCA.														
Version	1.11														
Referred by	Test case EAC2 ISO7816 J 52														
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>As defined by the CVCA</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETTESTDVDE014</td></tr> <tr> <td>Certificate Holder Authorization</td><td>domestic DV, DG 3, DG4</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 1 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair DV_KEY_14a</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_00</td></tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETTESTDVDE014	Certificate Holder Authorization	domestic DV, DG 3, DG4	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_14a	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETTESTDVDE014														
Certificate Holder Authorization	domestic DV, DG 3, DG4														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_14a														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.14.2 DV_CERT_14b

ID	DV_CERT_14b
Purpose	<p>Certificate with a wrong (short) public key.</p> <p>For RSA profile, same Algorithm Identifier but PK.DVCA's modulus length is shorter than the CVCA's key modulus length.</p> <p>For ECDSA profile, same Algorithm Identifier but DVCA's domain parameters are different and have a shorter prime length than the CVCA's key. The hash algorithm should be adapted if necessary.</p>
Version	1.11

Referred by	Test case EAC2_ISO7816_J_51														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>As defined by the CVCA</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTDVDE014</td></tr> <tr> <td>Certificate Holder Authorization</td><td>domestic DV, DG 3, DG4</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 1 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair DV_KEY_14b</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_00</td></tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE014	Certificate Holder Authorization	domestic DV, DG 3, DG4	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_14b	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETESTDVDE014														
Certificate Holder Authorization	domestic DV, DG 3, DG4														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_14b														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.14.3 IS_CERT_14a

ID	IS_CERT_14a
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_14.
Version	1.11
Referred by	Test case EAC2_ISO7816_J_51
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p>

	<p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	DETESTDVDE014
	Certificate Holder Reference	DETESTISDE014
	Certificate Holder Authorization	IS, DG 3, DG 4
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 14 days
	Public Key reference	Public key of key pair IS_KEY_14a
	Signing Key reference	Signed with the private key of key pair DV_KEY_14b

2.4.14.4 IS_CERT_14b

ID	IS CERT 14b
Purpose	<p>Certificate with a wrong (short) Public key.</p> <p>For RSA profile, same Algorithm Identifier but IS key modulus length is shorter than the DVCA's key modulus length.</p> <p>For ECDSA profile, same Algorithm Identifier but IS key domain parameters are different and have a shorter prime length than the DVCA's key. The hash algorithm should be adapted if necessary.</p>
Version	1.11
Referred by	Test case EAC2 ISO7816 J 52
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 03 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference</p>

	yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)	
Parameter	Certification Authority Reference	DETTESTDVDE014
	Certificate Holder Reference	DETTESTISDE014
	Certificate Holder Authorization	IS, DG 3, DG 4
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 14 days
	Public Key reference	Public key of key pair IS_KEY_14b
	Signing Key reference	Signed with the private key of key pair DV_KEY_14a

2.4.15 Certificate Set 15

Deleted in version 1.1.

2.4.16 Certificate Set 16

Deleted in version 1.1.

2.4.17 Certificate Set 17

This certificate set consists of a regular certificate chain (DV -> AT) which is used for the tests regarding eID special functions. The DV certificate permits special eID functions while the terminal certificate may restrict this access. The DV certificate is an official domestic certificate.

2.4.17.1 DV_CERT_17

ID	DV CERT 17
Purpose	This certificate is a regular DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits access to all eID special functions. It also permits read access to DG1 for testing access permissions.
Version	EAC2_1.0
Referred by	Test case EAC2_ISO7816_L_17, Test case EAC2_ISO7816_L_18, Test case EAC2_ISO7816_L_19, Test case EAC2_ISO7816_L_20, Test case EAC2_ISO7816_L_21, Test case EAC2_ISO7816_L_22, Test case EAC2_ISO7816_L_23, Test case EAC2_ISO7816_L_24, Test case EAC2_ISO7816_L_25, Test case EAC2_ISO7816_L_26, Test case EAC2_ISO7816_L_27, Test case EAC2_ISO7816_L_28, Test case EAC2_ISO7816_M_6, Test case EAC2_ISO7816_O_9, Test case EAC2_ISO7816_O_10, Test case EAC2_ISO7816_O_11, Test case EAC2_ISO7816_O_12, Test case EAC2_ISO7816_P_15, Test case EAC2_ISO7816_P_16, Test case EAC2_ISO7816_P_17, Test case EAC2_ISO7816_P_18, Test case EAC2_ISO7816_Q_1, Test case EAC2_ISO7816_Q_2, Test case EAC2_ISO7816_Q_3, Test case EAC2_ISO7816_Q_4, Test case EAC2_ISO7816_Q_6,

Test plan for eID-Cards with EAC 2.0

	Test case EAC2_ISO7816_Q_7, Test case EAC2_ISO7816_Q_8, Test case EAC2_ISO7816_Q_10, Test case EAC2_ISO7816_Q_11, Test case EAC2_ISO7816_Q_12, Test case EAC2_ISO7816_Q_13, Test case EAC2_ISO7816_Q_15, Test case EAC2_ISO7816_R_1, Test case EAC2_ISO7816_R_3, Test case EAC2_ISO7816_R_5, Test case EAC2_ISO7816_R_6, Test case EAC2_ISO7816_V_1, Test case EAC2_ISO7816_V_2, Test case EAC2_ISO7816_V_3, Test case EAC2_ISO7816_V_4, Test case EAC2_ISO7816_V_5, Test case EAC2_ISO7816_V_6, Test case EAC2_ISO7816_V_7, Test case EAC2_ISO7816_V_8, Test case EAC2_ISO7816_V_9, Test case EAC2_ISO7816_V_10, Test case EAC2_ISO7816_V_11, Test case EAC2_ISO7816_V_12														
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 40 00 01 FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>As defined by the initial AT CVCA reference</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETTESTDVDE017</td></tr> <tr> <td>Certificate Holder Authorization</td><td>Official domestic DV, eID-Specials (all), DG1</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 1 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair DV_KEY_17</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_17</td></tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETTESTDVDE017	Certificate Holder Authorization	Official domestic DV, eID-Specials (all), DG1	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_17	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
Certification Authority Reference	As defined by the initial AT CVCA reference														
Certificate Holder Reference	DETTESTDVDE017														
Certificate Holder Authorization	Official domestic DV, eID-Specials (all), DG1														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_17														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17														
	Test case EAC2_ISO7816_Q_7, Test case EAC2_ISO7816_Q_8, Test case EAC2_ISO7816_Q_10, Test case EAC2_ISO7816_Q_11, Test case EAC2_ISO7816_Q_12, Test case EAC2_ISO7816_Q_13, Test case EAC2_ISO7816_Q_15, Test case EAC2_ISO7816_R_1, Test case EAC2_ISO7816_R_3, Test case EAC2_ISO7816_R_5, Test case EAC2_ISO7816_R_6, Test case EAC2_ISO7816_V_1, Test case EAC2_ISO7816_V_2, Test case EAC2_ISO7816_V_3, Test case EAC2_ISO7816_V_4, Test case EAC2_ISO7816_V_5, Test case EAC2_ISO7816_V_6, Test case EAC2_ISO7816_V_7, Test case EAC2_ISO7816_V_8, Test case EAC2_ISO7816_V_9, Test case EAC2_ISO7816_V_10, Test case EAC2_ISO7816_V_11, Test case EAC2_ISO7816_V_12														
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 40 00 01 FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>As defined by the initial AT CVCA reference</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETTESTDVDE017</td></tr> <tr> <td>Certificate Holder Authorization</td><td>Official domestic DV, eID-Specials (all), DG1</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 1 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair DV_KEY_17</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_17</td></tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETTESTDVDE017	Certificate Holder Authorization	Official domestic DV, eID-Specials (all), DG1	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_17	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
Certification Authority Reference	As defined by the initial AT CVCA reference														
Certificate Holder Reference	DETTESTDVDE017														
Certificate Holder Authorization	Official domestic DV, eID-Specials (all), DG1														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_17														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17														

2.4.17.2 DV_CERT_17a

ID	DV_CERT_17a
Purpose	This certificate is a regular DV certificate, which validity is adopted to be used after link

	certificates are imported. The certificate permits access to all eID special functions. It also permits read access to DG1 for testing access permissions.														
Version	Smart-eID														
Referred by	Test case EAC2 ISO7816 M 6														
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 40 00 01 FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>As defined by the initial AT CVCA reference</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTDVDE017</td></tr> <tr> <td>Certificate Holder Authorization</td><td>Official domestic DV, eID-Specials (all), DG1</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}+ 6 month</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff}+ 9 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair DV KEY_17</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_17 or CVCA_KEY_11a depending on the execution of IS or AT certificates before</td></tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTDVDE017	Certificate Holder Authorization	Official domestic DV, eID-Specials (all), DG1	Certificate effective date	CVCA _{eff} + 6 month	Certificate expiration date	CVCA _{eff} + 9 month	Public Key reference	Public key of key pair DV KEY_17	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17 or CVCA_KEY_11a depending on the execution of IS or AT certificates before
Certification Authority Reference	As defined by the initial AT CVCA reference														
Certificate Holder Reference	DETESTDVDE017														
Certificate Holder Authorization	Official domestic DV, eID-Specials (all), DG1														
Certificate effective date	CVCA _{eff} + 6 month														
Certificate expiration date	CVCA _{eff} + 9 month														
Public Key reference	Public key of key pair DV KEY_17														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17 or CVCA_KEY_11a depending on the execution of IS or AT certificates before														

2.4.17.3 AT_CERT_17a

ID	AT_CERT_17a
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_17. It encodes access rights for the eID special function “CAN allowed”. To test read access without PIN, access to DG1 is granted.
Version	EAC2 1.0
Referred by	Test case EAC2_ISO7816_L_23, Test case EAC2_ISO7816_Q_3, Test case EAC2_ISO7816_Q_12

Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 01 10 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>DETESTDVDE017</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTATDE017</td></tr> <tr> <td>Certificate Holder Authorization</td><td>Terminal, CAN allowed, read DG1</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 1 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair AT_KEY_17</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair DV_KEY_17</td></tr> </table>	Certification Authority Reference	DETESTDVDE017	Certificate Holder Reference	DETESTATDE017	Certificate Holder Authorization	Terminal, CAN allowed, read DG1	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair AT_KEY_17	Signing Key reference	Signed with the private key of key pair DV_KEY_17
Certification Authority Reference	DETESTDVDE017														
Certificate Holder Reference	DETESTATDE017														
Certificate Holder Authorization	Terminal, CAN allowed, read DG1														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair AT_KEY_17														
Signing Key reference	Signed with the private key of key pair DV_KEY_17														

2.4.17.4 AT_CERT_17b

ID	AT_CERT_17b
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_17. It encodes access rights for the eID special function "PIN Management". Special function "CAN allowed" is additionally set in order to enable an alternative PACE password for PIN management function "Activate PIN".
Version	EAC2_1.0
Referred by	Test case EAC2_ISO7816_L_25, Test case EAC2_ISO7816_L_26, Test case EAC2_ISO7816_P_15, Test case EAC2_ISO7816_P_16, Test case EAC2_ISO7816_P_17, Test case EAC2_ISO7816_P_18, Test case EAC2_ISO7816_O_12
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 </pre>

	<pre> 00 00 00 30 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> 5F 37 <i>ii jj</i> </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>
Parameter	Certification Authority Reference
	DETESTDVDE017
	Certificate Holder Reference
	DETESTATDE017
	Certificate Holder Authorization
	Terminal, PIN Management, CAN allowed
	CVCA _{eff}
Parameter	Certificate effective date
	CVCA _{eff} + 1 month
	Certificate expiration date
	Public key of key pair AT_KEY_17
	Public Key reference
	Signed with the private key of key pair DV_KEY_17
	Signing Key reference

2.4.17.5 AT_CERT_17c

ID	AT CERT 17c
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_17. It encodes access rights for the eID special function “RI”.
Version	EAC2 1.0
Referred by	Test case EAC2_ISO7816_L_21, Test case EAC2_ISO7816_L_22, Test case EAC2_ISO7816_O_11, Test case EAC2_ISO7816_R_1, Test case EAC2_ISO7816_R_3, Test case EAC2_ISO7816_R_5, Test case EAC2_ISO7816_R_6
Content definition	<pre> 7F 21 <i>aa</i> 7F 4E <i>bb</i> 5F 29 01 00 42 <i>cc dd</i> 7F 49 <i>ee ff</i> 5F 20 <i>xx yy</i> 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 00 04 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> 65 <i>kk kk</i> L₇₃ 06 09 04 00 7F 00 07 03 01 03 02 80 11 <i>mm</i> 5F 37 <i>ii jj</i> </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object</p>

	<p><i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>kk</i> is the encoded length of the certificate extension object, <i>ll</i> is the encoded length of the terminal sector hash <i>mm</i> is the placeholder for the terminal sector hash</p>	
Parameter	Certification Authority Reference	DETESTDVDE017
	Certificate Holder Reference	DETESTATDE017
	Certificate Holder Authorization	Terminal, RI
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair AT_KEY_17
	Signing Key reference	Signed with the private key of key pair DV_KEY_17

2.4.17.6 AT_CERT_17d

ID	AT_CERT_17d
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_17. It encodes access rights for the eID special function “Install Qualified Certificate”.
Version	EAC2_1.0
Referred by	Test case EAC2_ISO7816_L_18, Test case EAC2_ISO7816_L_20, Test case EAC2_ISO7816_L_22, Test case EAC2_ISO7816_L_24, Test case EAC2_ISO7816_L_27, Test case EAC2_ISO7816_L_28
Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 00 80 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference</p>

	<code>yy</code> is the placeholder for the Certificate Holder Reference (xx bytes) <code>gg</code> is the placeholder for the BCD encoded effective date of the certificate <code>hh</code> is the placeholder for the BCD encoded expiration date of the certificate <code>ii</code> is the encoded length of the certificates signature object, <code>jj</code> is the placeholder for the certificates signature (ii bytes)	
Parameter	Certification Authority Reference	DETESTDVDE017
	Certificate Holder Reference	DETESTATDE017
	Certificate Holder Authorization	Terminal, Install Qualified Certificate
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair AT_KEY_17
	Signing Key reference	Signed with the private key of key pair DV_KEY_17

2.4.17.7 AT_CERT_17e

ID	AT_CERT_17e	
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_17. It encodes access rights for the eID special function “Install Certificate”.	
Version	EAC2_1.0	
Referred by	Test case EAC2_ISO7816_Q_4	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 00 40 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj <p><code>aa</code> is the encoded combined length of certificate body and signature objects <code>bb</code> is the encoded length of the certificate body object <code>cc</code> is the encoded length of the Certification Authority Reference <code>dd</code> is the placeholder for the Certification Authority Reference (cc bytes) <code>ee</code> is the encoded length of the certificate's public key, <code>ff</code> is the placeholder for the certificate's public key bytes (ee bytes), <code>xx</code> is the encoded length of the Certificate Holder Reference <code>yy</code> is the placeholder for the Certificate Holder Reference (xx bytes) <code>gg</code> is the placeholder for the BCD encoded effective date of the certificate <code>hh</code> is the placeholder for the BCD encoded expiration date of the certificate <code>ii</code> is the encoded length of the certificates signature object, <code>jj</code> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference DETESTDVDE017 Certificate Holder Reference DETESTATDE017 Certificate Holder Authorization Terminal, Install Certificate Certificate effective date CVCA _{eff}	

Test plan for eID-Cards with EAC 2.0

Certificate expiration date	CVCA _{eff} + 1 month
Public Key reference	Public key of key pair AT_KEY_17
Signing Key reference	Signed with the private key of key pair DV_KEY_17

2.4.17.8 AT_CERT_17f

ID	AT_CERT_17f														
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_17. It encodes access rights for the eID special function “Age Verification”.														
Version	EAC2 1.0														
Referred by	Test case EAC2_ISO7816_L_17, Test case EAC2_ISO7816_O_9, Test case EAC2_ISO7816_Q_1, Test case EAC2_ISO7816_Q_2														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 00 01 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTDVDE017</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTATDE017</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Terminal, Age Verification</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff}+ 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair AT_KEY_17</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair DV_KEY_17</td> </tr> </table>	Certification Authority Reference	DETESTDVDE017	Certificate Holder Reference	DETESTATDE017	Certificate Holder Authorization	Terminal, Age Verification	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair AT_KEY_17	Signing Key reference	Signed with the private key of key pair DV_KEY_17
Certification Authority Reference	DETESTDVDE017														
Certificate Holder Reference	DETESTATDE017														
Certificate Holder Authorization	Terminal, Age Verification														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair AT_KEY_17														
Signing Key reference	Signed with the private key of key pair DV_KEY_17														

2.4.17.9 AT_CERT_17g

ID	AT_CERT_17g
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_17. It encodes access rights for the eID special function “Municipality ID Check”.

Version	EAC2 1.0														
Referred by	Test case EAC2_ISO7816_L_19, Test case EAC2_ISO7816_O_10, Test case EAC2_ISO7816_Q_6, Test case EAC2_ISO7816_Q_7, Test case EAC2_ISO7816_Q_8, Test case EAC2_ISO7816_Q_10, Test case EAC2_ISO7816_Q_11, Test case EAC2_ISO7816_Q_13, Test case EAC2_ISO7816_Q_15														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 00 02 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTDVDE017</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTATDE017</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Terminal, Municipality ID Check</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair AT_KEY_17</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair DV_KEY_17</td> </tr> </table>	Certification Authority Reference	DETESTDVDE017	Certificate Holder Reference	DETESTATDE017	Certificate Holder Authorization	Terminal, Municipality ID Check	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair AT_KEY_17	Signing Key reference	Signed with the private key of key pair DV_KEY_17
Certification Authority Reference	DETESTDVDE017														
Certificate Holder Reference	DETESTATDE017														
Certificate Holder Authorization	Terminal, Municipality ID Check														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair AT_KEY_17														
Signing Key reference	Signed with the private key of key pair DV_KEY_17														

2.4.17.10 AT_CERT_17h

ID	AT_CERT_17h
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_17. It encodes access rights for the eID special function “CAN allowed” and “Privileged Terminal”.
Version	EAC2 1.1
Referred by	Test case EAC2_ISO7816_L_37
Content definition	<p>7F 21 aa 7F 4E bb</p>

	<pre> 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 00 18 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre>
	<p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>

Parameter

Certification Authority Reference	DETESTDVDE017
Certificate Holder Reference	DETESTSTATDE017
Certificate Holder Authorization	Terminal, CAN allowed, Privileged Terminal
Certificate effective date	CVCA _{eff}
Certificate expiration date	CVCA _{eff} + 1 month
Public Key reference	Public key of key pair AT KEY_17
Signing Key reference	Signed with the private key of key pair DV KEY_17

2.4.17.11 AT_CERT_17i

ID	AT_CERT_17i
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_17. It encodes access rights for the eID special function “PSA allowed” and “Privileged Terminal” and a sector public key.
Version	EAC2_1.1
Referred by	, Test case EAC2_ISO7816_V_1, Test case EAC2_ISO7816_V_2, Test case EAC2_ISO7816_V_3, Test case EAC2_ISO7816_V_4, Test case EAC2_ISO7816_V_5, Test case EAC2_ISO7816_V_6, Test case EAC2_ISO7816_V_7, Test case EAC2_ISO7816_V_8, Test case EAC2_ISO7816_V_9, Test case EAC2_ISO7816_V_10, Test case EAC2_ISO7816_V_11, Test case EAC2_ISO7816_V_12
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 </pre>

	<pre> 40 00 00 08 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> 65 <i>kk</i> 73 <i>L₇₃</i> 06 09 04 00 7F 00 07 03 01 03 03 A0 <i>L_{A0}</i> 80 11 <i>mm</i> 81 <i>nn</i> <i>oo</i> 5F 37 <i>ii jj</i> </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>kk</i> is the encoded length of the certificate extension object, <i>ll</i> is the encoded length of a domain parameter ID <i>mm</i> is the placeholder for the domain parameter ID <i>nn</i> is the encoded length of a sector public key hash <i>oo</i> is the placeholder for the second sector public key hash </p>
Parameter	Certification Authority Reference
	DETESTDVDE017
	Certificate Holder Reference
	DETESTATDE017
	Certificate Holder Authorization
	Terminal, PSA allowed, Privileged Terminal
	Certificate effective date
	CVCA _{eff}
	Certificate expiration date
	CVCA _{eff} + 1 month
	Public Key reference
	Public key of key pair AT_KEY_17
	Signing Key reference
	Signed with the private key of key pair DV_KEY_17

2.4.17.12 AT_CERT_17j

ID	AT_CERT_17j
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_17. It encodes access rights for the eID special functions “Age Verification” and “Municipality ID Check”.
Version	EAC2_1.1
Referred by	Test case EAC2_ISO7816_Q_18, EAC_ISO7816_U_9, EAC_ISO7816_U_10, EAC_ISO7816_U_11, EAC_ISO7816_U_12, EAC_ISO7816_U_13, EAC_ISO7816_U_14
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00

	<pre> 00 00 00 03 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> 5F 37 <i>ii jj</i> </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>
Parameter	Certification Authority Reference
	DETESTDVDE017
	Certificate Holder Reference
	DETESTSTATDE017
	Certificate Holder Authorization
	Terminal, Age Verification, Municipality ID Check
	Certificate effective date
	CVCA _{eff}
	Certificate expiration date
	CVCA _{eff} + 1 month
	Public Key reference
	Public key of key pair AT_KEY_17
	Signed with the private key of key pair DV_KEY_17

2.4.18 Certificate Set 18

This certificate set consists of a regular certificate chain (DV -> AT) which is used for the tests regarding eID special functions. The DV certificate permits special eID functions while the terminal certificate may restrict this access. The DV certificate is a non-official certificate.

2.4.18.1 DV_CERT_18

ID	DV CERT 18
Purpose	This certificate is a non-official DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits access to all eID special functions.
Version	EAC2_1.0
Referred by	Test case EAC2_ISO7816_Q_5, Test case EAC2_ISO7816_Q_9, Test case EAC2_ISO7816_Q_14, Test case EAC2_ISO7816_Q_16, Test case EAC2_ISO7816_R_8
Content definition	<pre> 7F 21 <i>aa</i> 7F 4E <i>bb</i> 5F 29 01 00 42 <i>cc dd</i> 7F 49 <i>ee ff</i> 5F 20 <i>xx yy</i> 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 40 40 00 00 FF </pre>

	<p style="text-align: center;"> 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </p> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>
Parameter	Certification Authority Reference
	As defined by the initial AT CVCA reference
	Certificate Holder Reference
	DETESTDVDE018
	Certificate Holder Authorization
	non-official DV, eID-Specials (all)
	CVCA _{eff}
Parameter	Certificate effective date
	CVCA _{eff} + 1 month
	Certificate expiration date
	Public key of key pair DV_KEY_18
	Public Key reference
	Signed with the private key of key pair CVCA_KEY_17
	Signing Key reference

2.4.18.2 AT_CERT_18a

ID	AT_CERT_18a
Version	deleted in version 1.00

2.4.18.3 AT_CERT_18b

ID	AT_CERT_18b
Version	deleted in version 1.00

2.4.18.4 AT_CERT_18c

ID	AT_CERT_18c
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_18. It encodes access rights for the eID special function “RI”.
Version	EAC2 1.0
Referred by	Test case EAC2 ISO7816 R 8
Content definition	<p style="text-align: center;"> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 </p>

	<pre> 00 00 00 04 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> 65 <i>kk</i> 73 L₇₃ 06 09 04 00 7F 00 07 03 01 03 02 80 11 <i>mm</i> 5F 37 <i>ii jj</i> </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>kk</i> is the encoded length of the certificate extension object, <i>ll</i> is the encoded length of the terminal sector hash <i>mm</i> is the placeholder for the terminal sector hash </p>
Parameter	Certification Authority Reference
	DETESTDVDE018
	Certificate Holder Reference
	DETESTATDE018
	Certificate Holder Authorization
	Authentication Terminal, RI
	Certificate effective date

2.4.18.5 AT_CERT_18d

ID	AT_CERT_18d
Version	deleted in version 1.00

2.4.18.6 AT_CERT_18e

ID	AT_CERT_18e
Version	deleted in version 1.00

2.4.18.7 AT_CERT_18f

ID	AT_CERT_18f
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_18. It encodes access rights for the eID special function “Age Verification”.
Version	EAC2_1.0
Referred by	Test case EAC2_ISO7816_Q_5
Content definition	7F 21 aa

	<pre> 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 00 01 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>
Parameter	Certification Authority Reference
	DETESTDVDE018
	Certificate Holder Reference
	DETESTSTATDE018
	Certificate Holder Authorization
	Terminal, Age Verification
	CVCA _{eff}
Parameter	Certificate effective date
	CVCA _{eff} + 1 month
	Certificate expiration date
	Public key of key pair AT_KEY_18
	Public Key reference
	Signed with the private key of key pair DV_KEY_18
	Signing Key reference

2.4.18.8 AT_CERT_18g

ID	AT_CERT_18g
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_18. It encodes access rights for the eID special function "Municipality ID Check".
Version	EAC2_1.0
Referred by	Test case EAC2_ISO7816_Q_9, Test case EAC2_ISO7816_Q_14, Test case EAC2_ISO7816_Q_16
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 00 02 5F 25 06 gg 5F 24 06 hh </pre>

	5F 37 ii jj
	<p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>
Parameter	Certification Authority Reference DETESTDVDE018
	Certificate Holder Reference DETESTATDE018
	Certificate Holder Authorization Terminal, Municipality ID Check
	Certificate effective date CVCA _{eff}
	Certificate expiration date CVCA _{eff} + 1 month
	Public Key reference Public key of key pair AT_KEY_18
	Signing Key reference Signed with the private key of key pair DV_KEY_18

2.4.19 Certificate Set 19

This certificate set consists of a regular certificate chain (DV > AT) which is used for the tests regarding eID read access. The DV certificate permits read access to all elementary files while the terminal certificate may restrict this access. The DV certificate is an official domestic certificate.

2.4.19.1 DV_CERT_19

ID	DV_CERT_19
Purpose	This certificate is a regular DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits read access to all elementary files
Version	EAC2 1.0
Referred by	Test case EAC2_ISO7816_K_14b, Test case EAC2_ISO7816_L_13 Template, Test case EAC2_ISO7816_L_15 Template , Test case EAC2_ISO7816_L16 Template, Test case EAC2_ISO7816_O_5 Template
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 3F FF FF 10 5F 25 06 gg 5F 24 06 hh

	5F 37 ii jj
<p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference
	As defined by the initial AT CVCA reference
	Certificate Holder Reference
	DETESTDVDE019
	Certificate Holder Authorization
	Official domestic DV, Read Access (all), CAN allowed
	Certificate effective date
	CVCA _{eff}
	Certificate expiration date
	CVCA _{eff} + 1 month
	Public Key reference
	Public key of key pair DV_KEY_19
	Signing Key reference
	Signed with the private key of key pair CVCA_KEY_17

2.4.19.2 DV_CERT_19a

ID	DV_CERT_19a
Purpose	This certificate is a regular DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits read access to all elementary files. It is a copy of DV_CERT_19 with the exception that all RFU bits within CHAT are set to 1.
Version	EAC2_1.0
Referred by	Test case EAC2 ISO7816 L_36
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 BF FF FF 10 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes)</p>

	ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)	
Parameter	Certification Authority Reference	As defined by the initial AT CVCA reference
	Certificate Holder Reference	DETTESTDVDE019
	Certificate Holder Authorization	Official domestic DV, Read Access (all), RFU=1, CAN allowed
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair DV KEY_19
	Signing Key reference	Signed with the private key of key pair CVCA KEY_17

2.4.19.3 AT_CERT_19_Template

ID	AT_CERT_19_template
Purpose	This certificate defines a template of a regular terminal certificate, which is issued by the DV CERT 19. The access rights are defined in a separate table
Version	see Table 1
Referred by	see Table 1
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 <AC-DO> 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj <p> aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes) $<AC-DO>$ is the access conditions data object as defined in Table 1 </p>

Parameter	Certification Authority Reference	DETESTDVDE019
	Certificate Holder Reference	DETESTATDE019
	Certificate Holder Authorization	see Table 1, column CHA, CAN allowed
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair AT_KEY_19
	Signing Key reference	Signed with the private key of key pair DV_KEY_19

2.4.19.4 AT_CERT_19a to AT_CERT_19w

ID	Purpose	Version	Referred by	AC-DO	CHA
AT_CERT_19a	Read access DG1	EAC2_1.0	EAC2_ISO7816_K_14b EAC2_ISO7816_L_13a	53 05 00 00 00 01 10	Terminal, read DG1
AT_CERT_19b	Read access DG2	EAC2_1.0	EAC2_ISO7816_L_13b	53 05 00 00 00 02 10	Terminal, read DG2
AT_CERT_19c	Read access DG3	EAC2_1.0	EAC2_ISO7816_L_13c	53 05 00 00 00 04 10	Terminal, read DG3
AT_CERT_19d	Read access DG4	EAC2_1.0	EAC2_ISO7816_L_13d	53 05 00 00 00 08 10	Terminal, read DG4
AT_CERT_19e	Read access DG5	EAC2_1.0	EAC2_ISO7816_L_13e	53 05 00 00 00 10 10	Terminal, read DG5
AT_CERT_19f	Read access DG6	EAC2_1.0	EAC2_ISO7816_L_13f	53 05 00 00 00 20 10	Terminal, read DG6
AT_CERT_19g	Read access DG7	EAC2_1.0	EAC2_ISO7816_L_13g	53 05 00 00 00 40 10	Terminal, read DG7
AT_CERT_19h	Read access DG8	EAC2_1.0	EAC2_ISO7816_L_13h	53 05 00 00 00 80 10	Terminal, read DG8
AT_CERT_19i	Read access DG9	EAC2_1.0	EAC2_ISO7816_L_13i	53 05 00 00 01 00 10	Terminal, read DG9
AT_CERT_19j	Read access DG10	EAC2_1.0	EAC2_ISO7816_L_13j	53 05 00 00 02 00 10	Terminal, read DG10
AT_CERT_19k	Read access DG11	EAC2_1.0	EAC2_ISO7816_L_13k	53 05 00 00 04 00 10	Terminal, read DG11
AT_CERT_19l	Read access DG12	EAC2_1.0	EAC2_ISO7816_L_13l	53 05 00 00 08 00 10	Terminal, read DG12
AT_CERT_19m	Read access DG13	EAC2_1.0	EAC2_ISO7816_L_13m	53 05 00 00 10 00 10	Terminal, read DG13
AT_CERT_19n	Read access DG14	EAC2_1.0	EAC2_ISO7816_L_13n	53 05 00 00 20 00 10	Terminal, read DG14
AT_CERT_19o	Read access DG15	EAC2_1.0	EAC2_ISO7816_L_13o	53 05 00 00 40 00 10	Terminal, read DG15
AT_CERT_19p	Read access DG16	EAC2_1.0	EAC2_ISO7816_L_13p	53 05 00 00 80 00 10	Terminal, read DG16
AT_CERT_19q	Read access DG17	EAC2_1.0	EAC2_ISO7816_L_13q, EAC2_ISO7816_L_15q, EAC2_ISO7816_L_16q	53 05 00 01 00 00 10	Terminal, read DG17

Test plan for eID Cards with EAC 2.0

ID	Purpose	Version	Referred by	AC-DO	CHA
AT_CERT_19r	Read access DG18	EAC2_1.0	EAC2_ISO7816_L_13r, EAC2_ISO7816_L_15r, EAC2_ISO7816_L_16r	53 05 00 02 00 00 10	Terminal, read DG18
AT_CERT_19s	Read access DG19	EAC2_1.0	EAC2_ISO7816_L_13s, EAC2_ISO7816_L_15s, EAC2_ISO7816_L_16s	53 05 00 04 00 00 10	Terminal, read DG19
AT_CERT_19t	Read access DG20	EAC2_1.0	EAC2_ISO7816_L_13t, EAC2_ISO7816_L_15t, EAC2_ISO7816_L_16t	53 05 00 08 00 00 10	Terminal, read DG20
AT_CERT_19u	Read access DG21	EAC2_1.0	EAC2_ISO7816_L_13u, EAC2_ISO7816_L_15u, EAC2_ISO7816_L_16u	53 05 00 10 00 00 10	Terminal, read DG21
AT_CERT_19v	Read access DG22	EAC2_1.1	EAC2_ISO7816_L_13v, EAC2_ISO7816_L_15v, EAC2_ISO7816_L_16v	53 05 00 20 00 00 10	Terminal, read DG22
AT_CERT_19w	Read access DG1	EAC2_1.0	EAC2_ISO7816_L_36	53 05 00 80 00 01 10	Terminal, read DG1, RFU=1

Table 1: Authorization of Authentication Terminals, Certificate issued by DV_CERT_19

2.4.20 Certificate Set 20

This certificate set consists of a regular certificate chain (DV -> AT) which is used for the tests regarding eID read access. The DV certificate permits read access to all elementary files while the terminal certificate may restrict this access. The DV certificate is a non-official certificate.

2.4.20.1 DV_CERT_20

ID	DV CERT 20														
Purpose	This certificate is a non-official DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits read access to all elementary files														
Version	EAC2_1.0														
Referred by	Test case EAC2_ISO7816_L_14 Template, Test case EAC2_ISO7816_O_6 Template														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 40 3F FF FF 00 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the initial AT CVCA reference</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE020</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>non-official DV</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_20</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_17</td> </tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTDVDE020	Certificate Holder Authorization	non-official DV	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_20	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
Certification Authority Reference	As defined by the initial AT CVCA reference														
Certificate Holder Reference	DETESTDVDE020														
Certificate Holder Authorization	non-official DV														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_20														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17														

2.4.20.2 DV_CERT_20a

ID	DV_CERT_20a															
Purpose	This certificate is a non-official DV certificate, which validity period is adopted for test suite M. The certificate permits read access to all elementary files															
Version	Smart-eID															
Referred by	Test case EAC2_ISO7816_M_9, Test case EAC2_ISO7816_M_10, Test case EAC2_ISO7816_M_11															
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 40 3F FF FF 00 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>															
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the initial AT CVCA reference</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE020</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>non-official DV</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff} + 5 months – 1 day</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 8 months</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_20</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_17</td> </tr> </table>		Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTDVDE020	Certificate Holder Authorization	non-official DV	Certificate effective date	CVCA _{eff} + 5 months – 1 day	Certificate expiration date	CVCA _{eff} + 8 months	Public Key reference	Public key of key pair DV_KEY_20	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
Certification Authority Reference	As defined by the initial AT CVCA reference															
Certificate Holder Reference	DETESTDVDE020															
Certificate Holder Authorization	non-official DV															
Certificate effective date	CVCA _{eff} + 5 months – 1 day															
Certificate expiration date	CVCA _{eff} + 8 months															
Public Key reference	Public key of key pair DV_KEY_20															
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17															

2.4.20.3 AT_CERT_20_Template

ID	AT_CERT_20a
Purpose	This certificate defines a template of a regular terminal certificate, which is issued by the DV_CERT_20. The access rights are defined in a separate table.
Version	see Table 2
Referred by	see Table 2

Test plan for eID-Cards with EAC 2.0

Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 <AC-DO> 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i><AC-DO></i> is the access conditions data object as defined in Table 2</p>
Parameter	Certification Authority Reference
	DETESTDVDE020
	Certificate Holder Reference
	DETESTATDE020
	Certificate Holder Authorization
	See Table 2, column CHA
	Certificate effective date

2.4.20.4 AT_CERT_20a to AT_CERT_20v

ID	Purpose	Version	Referred by	AC-DO	CHA
AT_CERT_20a	Read access DG1	EAC2_1.0	EAC2_ISO7816_L_14a	53 05 00 00 00 01 00	Terminal, read DG1
AT_CERT_20b	Read access DG2	EAC2_1.0	EAC2_ISO7816_L_14b	53 05 00 00 00 02 00	Terminal, read DG2
AT_CERT_20c	Read access DG3	EAC2_1.0	EAC2_ISO7816_L_14c	53 05 00 00 00 04 00	Terminal, read DG3
AT_CERT_20d	Read access DG4	EAC2_1.0	EAC2_ISO7816_L_14d	53 05 00 00 00 08 00	Terminal, read DG4
AT_CERT_20e	Read access DG5	EAC2_1.0	EAC2_ISO7816_L_14e	53 05 00 00 00 10 00	Terminal, read DG5
AT_CERT_20f	Read access DG6	EAC2_1.0	EAC2_ISO7816_L_14f	53 05 00 00 00 20 00	Terminal, read DG6
AT_CERT_20g	Read access DG7	EAC2_1.0	EAC2_ISO7816_L_14g	53 05 00 00 00 40 00	Terminal, read DG7
AT_CERT_20h	Read access DG8	EAC2_1.0	EAC2_ISO7816_L_14h	53 05 00 00 00 80 00	Terminal, read DG8
AT_CERT_20i	Read access DG9	EAC2_1.0	EAC2_ISO7816_L_14i	53 05 00 00 01 00 00	Terminal, read DG9
AT_CERT_20j	Read access DG10	EAC2_1.0	EAC2_ISO7816_L_14j	53 05 00 00 02 00 00	Terminal, read DG10
AT_CERT_20k	Read access DG11	EAC2_1.0	EAC2_ISO7816_L_14k	53 05 00 00 04 00 00	Terminal, read DG11
AT_CERT_20l	Read access DG12	EAC2_1.0	EAC2_ISO7816_L_14l	53 05 00 00 08 00 00	Terminal, read DG12
AT_CERT_20m	Read access DG13	EAC2_1.0	EAC2_ISO7816_L_14m	53 05 00 00 10 00 00	Terminal, read DG13
AT_CERT_20n	Read access DG14	EAC2_1.0	EAC2_ISO7816_L_14n	53 05 00 00 20 00 00	Terminal, read DG14
AT_CERT_20o	Read access DG15	EAC2_1.0	EAC2_ISO7816_L_14o	53 05 00 00 40 00 00	Terminal, read DG15
AT_CERT_20p	Read access DG16	EAC2_1.0	EAC2_ISO7816_L_14p	53 05 00 00 80 00 00	Terminal, read DG16
AT_CERT_20q	Read access DG17	EAC2_1.0	EAC2_ISO7816_L_14q	53 05 00 01 00 00 00	Terminal, read DG17
AT_CERT_20r	Read access DG18	EAC2_1.0	EAC2_ISO7816_L_14r	53 05 00 02 00 00 00	Terminal, read DG18
AT_CERT_20s	Read access DG19	EAC2_1.0	EAC2_ISO7816_L_14s	53 05 00 04 00 00 00	Terminal, read DG19
AT_CERT_20t	Read access DG20	EAC2_1.0	EAC2_ISO7816_L_14t	53 05 00 08 00 00 00	Terminal, read DG20
AT_CERT_20u	Read access DG21	EAC2_1.0	EAC2_ISO7816_L_14u	53 05 00 10 00 00 00	Terminal, read DG21
AT_CERT_20v	Read access DG22	EAC2_1.1	EAC2_ISO7816_L_14v	53 05 00 20 00 00 00	Terminal, read DG22

Table 2: Authorization of Authentication Terminals, Certificate issued by DV_CERT_20

2.4.20.5 AT_CERT_20w

ID	AT_CERT_20w														
Purpose	This certificate defines a regular terminal certificate, which is issued by the DV_CERT_20..														
Version	Smart-eID														
Referred by	Test case EAC2_ISO7816_M_9, Test case EAC2_ISO7816_M_10, Test case EAC2_ISO7816_M_11														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 01 00 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i><AC-DO></i> is the access conditions data object as defined in Table 2</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>DETESTDVDE020</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTATDE020</td></tr> <tr> <td>Certificate Holder Authorization</td><td>Terminal, read DG1</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff} + 5 month – 1 day</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 8 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair AT_KEY_20</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair DV_KEY_20</td></tr> </table>	Certification Authority Reference	DETESTDVDE020	Certificate Holder Reference	DETESTATDE020	Certificate Holder Authorization	Terminal, read DG1	Certificate effective date	CVCA _{eff} + 5 month – 1 day	Certificate expiration date	CVCA _{eff} + 8 month	Public Key reference	Public key of key pair AT_KEY_20	Signing Key reference	Signed with the private key of key pair DV_KEY_20
Certification Authority Reference	DETESTDVDE020														
Certificate Holder Reference	DETESTATDE020														
Certificate Holder Authorization	Terminal, read DG1														
Certificate effective date	CVCA _{eff} + 5 month – 1 day														
Certificate expiration date	CVCA _{eff} + 8 month														
Public Key reference	Public key of key pair AT_KEY_20														
Signing Key reference	Signed with the private key of key pair DV_KEY_20														

2.4.21 Certificate Set 21

This certificate set consists of a regular certificate chain (DV -> AT) which is used for the tests regarding eID write access. The DV certificate permits write access to all elementary files while the terminal certificate may restrict this access. The DV certificate is an official domestic certificate.

2.4.21.1 DV_CERT_21

ID	DV_CERT_21															
Purpose	This certificate is a regular DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits write access to all elementary files															
Version	EAC2_1.0															
Referred by	Test case EAC2_ISO7816_L_15 Template, Test case EAC2_ISO7816_O_7 Template															
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 BF 00 00 00 10 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>															
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the initial AT CVCA reference</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE021</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Official domestic DV, write access (all), CAN allowed</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_21</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_17</td> </tr> </table>		Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTDVDE021	Certificate Holder Authorization	Official domestic DV, write access (all), CAN allowed	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_21	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
Certification Authority Reference	As defined by the initial AT CVCA reference															
Certificate Holder Reference	DETESTDVDE021															
Certificate Holder Authorization	Official domestic DV, write access (all), CAN allowed															
Certificate effective date	CVCA _{eff}															
Certificate expiration date	CVCA _{eff} + 1 month															
Public Key reference	Public key of key pair DV_KEY_21															
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17															

2.4.21.2 AT_CERT_21_Template

ID	AT_CERT_21_template
Purpose	This certificate defines a template of a regular terminal certificate, which is issued by the DV_CERT_21. The access rights are defines in a separate table
Version	See Table 3
Referred by	See Table 3

Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 <AC-DO> 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <AC-DO> are the access conditions as defined in Table 3</p>
Parameter	Certification Authority Reference
	DETESTDVDE021
	Certificate Holder Reference
	DETESTATDE021
	Certificate Holder Authorization
	See Table 3, column CHA, CAN allowed
	Certificate effective date

2.4.21.3 AT_CERT_21a to AT_CERT_21f

ID	Purpose	Version	Referred by	AC-DO	CHA
AT_CERT_21a	R/W access DG17	EAC2 1.03	EAC2 ISO7816 L 15a	53 05 20 00 00 00 10	Terminal, r/w DG17
AT_CERT_21b	R/W access DG18	EAC2 1.03	EAC2 ISO7816 L 15b	53 05 10 00 00 00 10	Terminal, r/w DG18
AT_CERT_21c	R/W access DG19	EAC2 1.03	EAC2 ISO7816 L 15c	53 05 08 00 00 00 10	Terminal, r/w DG19
AT_CERT_21d	R/W access DG20	EAC2 1.03	EAC2 ISO7816 L 15d	53 05 04 00 00 00 10	Terminal, r/w DG20
AT_CERT_21e	R/W access DG21	EAC2 1.03	EAC2 ISO7816 L 15e	53 05 02 00 00 00 10	Terminal, r/w DG21
AT_CERT_21f	R/W access DG22	EAC2 1.1	EAC2 ISO7816 L 15f	53 05 01 0 00 00 10	Terminal, r/w DG22

Table 3: Authorization of Authentication Terminals, Certificate issued by DV_CERT_21

2.4.22 Certificate Set 22

This certificate set consists of a regular certificate chain (DV -> AT) which is used for the tests regarding eID write access. The DV certificate permits write access to all elementary files while the terminal certificate may restrict this access. The DV certificate is a non-official certificate.

2.4.22.1 DV_CERT_22

ID	DV CERT 22														
Purpose	This certificate is a non-official DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits write access to all elementary files														
Version	EAC2_1.0														
Referred by	Test case EAC2_ISO7816_L_16 Template, Test case EAC2_ISO7816_O_8 Template														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 7F 00 00 00 00 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the initial AT CVCA reference</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE022</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>non-official DV, write access (all)</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_22</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_17</td> </tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTDVDE022	Certificate Holder Authorization	non-official DV, write access (all)	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_22	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
Certification Authority Reference	As defined by the initial AT CVCA reference														
Certificate Holder Reference	DETESTDVDE022														
Certificate Holder Authorization	non-official DV, write access (all)														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_22														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17														

2.4.22.2 AT_CERT_22_Template

ID	AT_CERT_22a														
Purpose	This certificate defines a template of a regular terminal certificate, which is issued by the DV_CERT_22. The access rights are defined in a separate table.														
Version	See Table 4														
Referred by	See Table 4														
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 <AC-DO> 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i><AC-DO></i> are the access conditions as defined in Table 4 </p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTDVDE022</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTSTATDE022</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Table 4, column CHA</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair AT_KEY_22</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair DV_KEY_22</td> </tr> </table>	Certification Authority Reference	DETESTDVDE022	Certificate Holder Reference	DETESTSTATDE022	Certificate Holder Authorization	Table 4, column CHA	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair AT_KEY_22	Signing Key reference	Signed with the private key of key pair DV_KEY_22
Certification Authority Reference	DETESTDVDE022														
Certificate Holder Reference	DETESTSTATDE022														
Certificate Holder Authorization	Table 4, column CHA														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair AT_KEY_22														
Signing Key reference	Signed with the private key of key pair DV_KEY_22														

2.4.22.3 AT_CERT_22a to AT_CERT_22f

ID	Purpose	Version	Referred by	AC-DO	CHA
AT_CERT_22a	R/W access DG17	EAC2 1.03	EAC2 ISO7816 L 16a	53 05 20 00 00 00 00	Terminal, r/w DG17
AT_CERT_22b	R/W access DG18	EAC2 1.03	EAC2 ISO7816 L 16b	53 05 10 00 00 00 00	Terminal, r/w DG18
AT_CERT_22c	R/W access DG19	EAC2 1.03	EAC2 ISO7816 L 16c	53 05 08 00 00 00 00	Terminal, r/w DG19
AT_CERT_22d	R/W access DG20	EAC2 1.03	EAC2 ISO7816 L 16d	53 05 04 00 00 00 00	Terminal, r/w DG20
AT_CERT_22e	R/W access DG21	EAC2 1.03	EAC2 ISO7816 L 16e	53 05 02 00 00 00 00	Terminal, r/w DG21
AT_CERT_22f	R/W access DG22	EAC2 1.1	EAC2 ISO7816 L 16f	53 05 01 00 00 00 00	Terminal, r/w DG22

Table 4: Authorization of Authentication Terminals, Certificate issued by DV_CERT_22

2.4.23 Certificate Set 23

This certificate set defines a link certificate used for the tests about the trust point update mechanism.

2.4.23.1 LINK_CERT_23a

ID	LINK CERT 23a														
Purpose	This certificate is a link certificate, which validity period starts one month before the original CVCA certificate expires.														
Version	EAC2 1.0														
Referred by	Test case EAC2 ISO7816 M 7														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 FF 7F FF FF FF 5F 25 06 gg 5F 24 06 hh <i>optional:</i> 65 vv ww 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>vv</i> is the encoded length of the certificate extension, <i>ww</i> is the placeholder for the certificate extension (vv bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the initial AT CVCA reference</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTLINKDE23A</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>CVCA, read access to all DG, all eID functions</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{exp} + 2 months</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{exp} + 5 months</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair AT CVCA KEY 23a</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_17 or CVCA_KEY_11a depending on the execution of IS or AT certificates before</td> </tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTLINKDE23A	Certificate Holder Authorization	CVCA, read access to all DG, all eID functions	Certificate effective date	CVCA _{exp} + 2 months	Certificate expiration date	CVCA _{exp} + 5 months	Public Key reference	Public key of key pair AT CVCA KEY 23a	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17 or CVCA_KEY_11a depending on the execution of IS or AT certificates before
Certification Authority Reference	As defined by the initial AT CVCA reference														
Certificate Holder Reference	DETESTLINKDE23A														
Certificate Holder Authorization	CVCA, read access to all DG, all eID functions														
Certificate effective date	CVCA _{exp} + 2 months														
Certificate expiration date	CVCA _{exp} + 5 months														
Public Key reference	Public key of key pair AT CVCA KEY 23a														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17 or CVCA_KEY_11a depending on the execution of IS or AT certificates before														

	Certificate Extension	As defined by CVCA
--	-----------------------	--------------------

2.4.23.2 LINK_CERT_23b

ID	LINK_CERT_23b																	
Purpose	This certificate is a link certificate, which validity period starts one month before the previous CVCA certificate expires.																	
Version	EAC2_1.0																	
Referred by	Test case EAC2 ISO7816 M 7																	
Content definition	<p> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 FF 7F FF FF FF 5F 25 06 gg 5F 24 06 hh <i>optional:</i> 65 vv ww 5F 37 ii jj </p> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>vv</i> is the encoded length of the certificate extension, <i>ww</i> is the placeholder for the certificate extension (vv bytes) </p>																	
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTLINKDE23A</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTLINKDE23B</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>CVCA, read access to all DG, all eID functions</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{exp} + 4 month</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{exp} + 7 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair AT_CVCA_KEY_23b</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair AT_CVCA_KEY_23a</td> </tr> <tr> <td>Certificate Extension</td> <td>As defined by CVCA</td> </tr> </table>		Certification Authority Reference	DETESTLINKDE23A	Certificate Holder Reference	DETESTLINKDE23B	Certificate Holder Authorization	CVCA, read access to all DG, all eID functions	Certificate effective date	CVCA _{exp} + 4 month	Certificate expiration date	CVCA _{exp} + 7 month	Public Key reference	Public key of key pair AT_CVCA_KEY_23b	Signing Key reference	Signed with the private key of key pair AT_CVCA_KEY_23a	Certificate Extension	As defined by CVCA
Certification Authority Reference	DETESTLINKDE23A																	
Certificate Holder Reference	DETESTLINKDE23B																	
Certificate Holder Authorization	CVCA, read access to all DG, all eID functions																	
Certificate effective date	CVCA _{exp} + 4 month																	
Certificate expiration date	CVCA _{exp} + 7 month																	
Public Key reference	Public key of key pair AT_CVCA_KEY_23b																	
Signing Key reference	Signed with the private key of key pair AT_CVCA_KEY_23a																	
Certificate Extension	As defined by CVCA																	

2.4.23.3 DV_CERT_23

ID	DV_CERT_23
----	------------

Purpose	This certificate is a domestic DV certificate, which was issued by the previous AT CVCA.														
Version	EAC2_1.0														
Referred by	Test case EAC2_ISO7816_M_7														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 3F FF FF 00 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>DETESTLINKDE23A</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTDVDE023</td></tr> <tr> <td>Certificate Holder Authorization</td><td>domestic DV, read access all DGs</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{exp} + 4 month</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{exp} + 5 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair DV_KEY_23</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair AT_CVCA_KEY_23a</td></tr> </table>	Certification Authority Reference	DETESTLINKDE23A	Certificate Holder Reference	DETESTDVDE023	Certificate Holder Authorization	domestic DV, read access all DGs	Certificate effective date	CVCA _{exp} + 4 month	Certificate expiration date	CVCA _{exp} + 5 month	Public Key reference	Public key of key pair DV_KEY_23	Signing Key reference	Signed with the private key of key pair AT_CVCA_KEY_23a
Certification Authority Reference	DETESTLINKDE23A														
Certificate Holder Reference	DETESTDVDE023														
Certificate Holder Authorization	domestic DV, read access all DGs														
Certificate effective date	CVCA _{exp} + 4 month														
Certificate expiration date	CVCA _{exp} + 5 month														
Public Key reference	Public key of key pair DV_KEY_23														
Signing Key reference	Signed with the private key of key pair AT_CVCA_KEY_23a														

2.4.24 Certificate Set 24

This certificate set consists of a regular certificate chain (DV -> AT) which is used for the tests regarding Restricted Identification. The DV certificate permits special eID functions while the terminal certificate may restrict this access. The DV certificate is an official domestic certificate.

2.4.24.1 DV_CERT_24

ID	DV_CERT_24
Purpose	This certificate is a official DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits RI special function.
Version	EAC2_1.0

Referred by	Test case EAC2_ISO7816_R_10, Test case EAC2_ISO7816_R_12														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 00 00 00 04 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>As defined by the initial AT CVCA reference</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTDVDE024</td></tr> <tr> <td>Certificate Holder Authorization</td><td>official DV, eID-Special RI</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 1 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair DV_KEY_24</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_17</td></tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTDVDE024	Certificate Holder Authorization	official DV, eID-Special RI	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_24	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
Certification Authority Reference	As defined by the initial AT CVCA reference														
Certificate Holder Reference	DETESTDVDE024														
Certificate Holder Authorization	official DV, eID-Special RI														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_24														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17														

2.4.24.2 AT_CERT_24

ID	AT_CERT_24
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_24. It encodes access rights for the eID special function “RI” and two sector public keys.
Version	EAC2_1.0
Referred by	Test case EAC2_ISO7816_R_10, Test case EAC2_ISO7816_R_12
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 00 00 00 04</p>

	<pre> 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> 65 <i>kk</i> 73 L₇₃ 06 09 04 00 7F 00 07 03 01 03 02 80 11 <i>mm</i> 81 11 <i>nn</i> 5F 37 <i>ii jj</i> </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>kk</i> is the encoded length of the certificate extension object, <i>ll</i> is the encoded length of a sector public key hash <i>mm</i> is the placeholder for the first sector public key hash <i>nn</i> is the placeholder for the second sector public key hash </p>
Parameter	Certification Authority Reference
	DETESTDVDE024
	Certificate Holder Reference
	DETESTATDE024
	Certificate Holder Authorization
	Terminal, RI
	Certificate effective date

2.4.25 Certificate Set 25

Deleted in version 1.00 RC

2.4.26 Certificate Set 26

Deleted in version 1.00 RC

2.4.27 Certificate Set 27

Deleted in version 1.1.

2.4.28 Certificate Set 28

Deleted in version 1.1.

2.4.29 Certificate Set 29

Deleted in version 1.1.

2.4.30 Certificate Set 30

The certificate set follows a certification scheme where the DV permits access to compare data groups. The right to compare data groups is encoded in additional Authorization Extensions.

2.4.30.1 DV_CERT_30

ID	DV CERT 30				
Purpose	This certificate is a regular DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits access to all eID special functions. It also permits compare access to DG1 to DG22 for testing compare permissions in Authorization Extensions.				
Version	EAC2_1.1				
Referred by	Test case EAC2_ISO7816_U_1_Template, Test case EAC2_ISO7816_U_2_Template, Test case EAC2_ISO7816_U_3_Template, Test case EAC2_ISO7816_U_4_Template				
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 80 06 00 00 00 3F FF FF 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Template <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>				
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>As defined by the initial AT CVCA reference</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETESTDVDE030</td></tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTDVDE030
Certification Authority Reference	As defined by the initial AT CVCA reference				
Certificate Holder Reference	DETESTDVDE030				

Certificate Holder Authorization	Official domestic DV, eID-Specials (all)
Certificate effective date	CVCA _{eff}
Certificate expiration date	CVCA _{eff} + 1 month
Public Key reference	Public key of key pair DV_KEY_30
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17

2.4.30.2 DV_CERT_30a

ID	DV CERT 30a												
Purpose	This certificate is a regular DV certificate, which is adopted for test suite M.												
Version	EAC2_1.1												
Referred by	Test case EAC2_ISO7816_M_12, Test case EAC2_ISO7816_M_13, Test case EAC2_ISO7816_M_14												
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 80 06 00 00 00 3F FF FF 5F 37 ii jj</p> <p>aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, kk is the encoded length of the certificate extension object ll is the encoded length of the Discretionary Data Template jj is the placeholder for the certificates signature (ii bytes)</p>												
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the initial AT CVCA reference</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE030</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Official domestic DV, eID-Specials (all)</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff} + 5 months – 1 day</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 8 months</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_30</td> </tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTDVDE030	Certificate Holder Authorization	Official domestic DV, eID-Specials (all)	Certificate effective date	CVCA _{eff} + 5 months – 1 day	Certificate expiration date	CVCA _{eff} + 8 months	Public Key reference	Public key of key pair DV_KEY_30
Certification Authority Reference	As defined by the initial AT CVCA reference												
Certificate Holder Reference	DETESTDVDE030												
Certificate Holder Authorization	Official domestic DV, eID-Specials (all)												
Certificate effective date	CVCA _{eff} + 5 months – 1 day												
Certificate expiration date	CVCA _{eff} + 8 months												
Public Key reference	Public key of key pair DV_KEY_30												

	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
--	-----------------------	--

2.4.30.3 AT_CERT_30_Template

ID	AT_CERT_30_template															
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_30. It encodes access rights for the eID special function “Compare DGx” in Authorization Extensions.															
Version	EAC2_1.1															
Referred by	Test case EAC2_ISO7816_U_1_Template, Test case EAC2_ISO7816_U_2_Template, Test case EAC2_ISO7816_U_3_Template, Test case EAC2_ISO7816_U_4_Template															
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 <Authorization Extension> 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>															
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTDVDE030</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTSTATDE030</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Terminal,</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair AT_KEY_30</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair DV_KEY_30</td> </tr> </table>		Certification Authority Reference	DETESTDVDE030	Certificate Holder Reference	DETESTSTATDE030	Certificate Holder Authorization	Terminal,	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair AT_KEY_30	Signing Key reference	Signed with the private key of key pair DV_KEY_30
Certification Authority Reference	DETESTDVDE030															
Certificate Holder Reference	DETESTSTATDE030															
Certificate Holder Authorization	Terminal,															
Certificate effective date	CVCA _{eff}															
Certificate expiration date	CVCA _{eff} + 1 month															
Public Key reference	Public key of key pair AT_KEY_30															
Signing Key reference	Signed with the private key of key pair DV_KEY_30															

2.4.30.4 AT_CERT_30a to AT_CERT_30w

Cert-ID	Version	Access Right	Authorization Extension
AT_CERT_30a	EAC2_1.1	Compare DG1	80 06 00 00 00 00 00 00 01
AT_CERT_30b	EAC2_1.1	Compare DG2	80 06 00 00 00 00 00 00 02
AT_CERT_30c	EAC2_1.1	Compare DG3	80 06 00 00 00 00 00 00 04
AT_CERT_30d	EAC2_1.1	Compare DG4	80 06 00 00 00 00 00 00 08
AT_CERT_30e	EAC2_1.1	Compare DG5	80 06 00 00 00 00 00 00 10
AT_CERT_30f	EAC2_1.1	Compare DG6	80 06 00 00 00 00 00 00 20
AT_CERT_30g	EAC2_1.1	Compare DG7	80 06 00 00 00 00 00 00 40
AT_CERT_30h	EAC2_1.1	Compare DG8	80 06 00 00 00 00 00 00 80
AT_CERT_30i	EAC2_1.1	Compare DG9	80 06 00 00 00 00 00 01 00
AT_CERT_30j	EAC2_1.1	Compare DG10	80 06 00 00 00 00 00 02 00
AT_CERT_30k	EAC2_1.1	Compare DG11	80 06 00 00 00 00 00 04 00
AT_CERT_30l	EAC2_1.1	Compare DG12	80 06 00 00 00 00 00 08 00
AT_CERT_30m	EAC2_1.1	Compare DG13	80 06 00 00 00 00 00 10 00
AT_CERT_30n	EAC2_1.1	Compare DG14	80 06 00 00 00 00 00 20 00
AT_CERT_30o	EAC2_1.1	Compare DG15	80 06 00 00 00 00 00 40 00
AT_CERT_30p	EAC2_1.1	Compare DG16	80 06 00 00 00 00 00 80 00
AT_CERT_30q	EAC2_1.1	Compare DG17	80 06 00 00 00 01 00 00
AT_CERT_30r	EAC2_1.1	Compare DG18	80 06 00 00 00 02 00 00
AT_CERT_30s	EAC2_1.1	Compare DG19	80 06 00 00 00 04 00 00
AT_CERT_30t	EAC2_1.1	Compare DG20	80 06 00 00 00 08 00 00
AT_CERT_30u	EAC2_1.1	Compare DG21	80 06 00 00 00 10 00 00
AT_CERT_30v	EAC2_1.1	Compare DG22	80 06 00 00 00 20 00 00
AT_CERT_30w	EAC2_1.1	No Compare	80 06 00 00 00 00 00 00 00

Table 5: Authorization Extension of AT_CERT_30

2.4.30.5 AT_CERT_30x

Deleted in version 1.3 RC 4

2.4.30.6 AT_CERT_30y

ID	AT_CERT_30y														
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_30. It is adopted for test suite M and including Compare DG8.														
Version	Smart-eID														
Referred by	Test case EAC2_ISO7816_M12, Test case EAC2_ISO7816_M13, Test case EAC2_ISO7816_M14														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 80 06 00 00 00 00 00 01 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTDVDE030</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTSTATDE030</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Authentication Terminal</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff} + 5 months – 1 day</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 8 months</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair AT_KEY_30</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair DV_KEY_30</td> </tr> </table>	Certification Authority Reference	DETESTDVDE030	Certificate Holder Reference	DETESTSTATDE030	Certificate Holder Authorization	Authentication Terminal	Certificate effective date	CVCA _{eff} + 5 months – 1 day	Certificate expiration date	CVCA _{eff} + 8 months	Public Key reference	Public key of key pair AT_KEY_30	Signing Key reference	Signed with the private key of key pair DV_KEY_30
Certification Authority Reference	DETESTDVDE030														
Certificate Holder Reference	DETESTSTATDE030														
Certificate Holder Authorization	Authentication Terminal														
Certificate effective date	CVCA _{eff} + 5 months – 1 day														
Certificate expiration date	CVCA _{eff} + 8 months														
Public Key reference	Public key of key pair AT_KEY_30														
Signing Key reference	Signed with the private key of key pair DV_KEY_30														

2.4.30.7 AT_CERT_30z

ID	AT_CERT_30z
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_30. It is adopted for test suite M and including Compare DG1.

Test plan for eID-Cards with EAC 2.0

Version	Smart-eID														
Referred by	Test case EAC2 ISO7816 M14														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 80 06 00 00 00 00 00 80 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>DETTESTDVDE030</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETTESTATDE030</td></tr> <tr> <td>Certificate Holder Authorization</td><td>Authentication Terminal</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff} + 5 months – 1 day</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 8 months</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair AT_KEY_30</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair DV_KEY_30</td></tr> </table>	Certification Authority Reference	DETTESTDVDE030	Certificate Holder Reference	DETTESTATDE030	Certificate Holder Authorization	Authentication Terminal	Certificate effective date	CVCA _{eff} + 5 months – 1 day	Certificate expiration date	CVCA _{eff} + 8 months	Public Key reference	Public key of key pair AT_KEY_30	Signing Key reference	Signed with the private key of key pair DV_KEY_30
Certification Authority Reference	DETTESTDVDE030														
Certificate Holder Reference	DETTESTATDE030														
Certificate Holder Authorization	Authentication Terminal														
Certificate effective date	CVCA _{eff} + 5 months – 1 day														
Certificate expiration date	CVCA _{eff} + 8 months														
Public Key reference	Public key of key pair AT_KEY_30														
Signing Key reference	Signed with the private key of key pair DV_KEY_30														

2.4.31 Certificate Set 31

The certificate set follows a certification scheme where the DV permits access to compare data groups.

2.4.31.1 DV_CERT_31

ID	DV_CERT_31
Purpose	This certificate is a non-official DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits access to all eID special functions. It also permits compare access to DG1 to DG22 for testing compare permissions in Authorization Extensions.

Version	EAC2_1.1														
Referred by	Test case EAC2_ISO7816_U_5_Template														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 40 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 80 06 00 00 00 3F FF FF 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td><td>As defined by the initial AT CVCA reference</td></tr> <tr> <td>Certificate Holder Reference</td><td>DETTESTDVDE030</td></tr> <tr> <td>Certificate Holder Authorization</td><td>Non-official domestic DV, eID-Specials (all)</td></tr> <tr> <td>Certificate effective date</td><td>CVCA_{eff}</td></tr> <tr> <td>Certificate expiration date</td><td>CVCA_{eff} + 1 month</td></tr> <tr> <td>Public Key reference</td><td>Public key of key pair DV_KEY_31</td></tr> <tr> <td>Signing Key reference</td><td>Signed with the private key of key pair CVCA_KEY_17</td></tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETTESTDVDE030	Certificate Holder Authorization	Non-official domestic DV, eID-Specials (all)	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_31	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
Certification Authority Reference	As defined by the initial AT CVCA reference														
Certificate Holder Reference	DETTESTDVDE030														
Certificate Holder Authorization	Non-official domestic DV, eID-Specials (all)														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_31														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17														

2.4.31.2 AT_CERT_31_Template

ID	AT_CERT_31_template
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_31. It encodes access rights for the eID special function “Compare DGx” in Authorization Extensions.
Version	EAC2_1.1
Referred by	Test case EAC2_ISO7816_U_5_Template
Content definition	7F 21 aa

	<pre> 7F 4E <i>bb</i> 5F 29 01 00 42 <i>cc dd</i> 7F 49 <i>ee ff</i> 5F 20 <i>xx yy</i> 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 7F FF FF FF 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> 65 <i>kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01</i> <Authorization Extension> 5F 37 <i>ii jj</i> </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	DETESTDVDE030
	Certificate Holder Reference	DETESTATDE030
	Certificate Holder Authorization	Terminal, Compare DGx
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair AT_KEY_30
	Signing Key reference	Signed with the private key of key pair DV_KEY_30

2.4.31.3 AT_CERT_31a to AT_CERT_31w

Cert-ID	Version	Access Right	Authorization Extension
AT_CERT_31a	EAC2_1.1	Compare DG1	80 06 00 00 00 00 00 00 01
AT_CERT_31b	EAC2_1.1	Compare DG2	80 06 00 00 00 00 00 00 02
AT_CERT_31c	EAC2_1.1	Compare DG3	80 06 00 00 00 00 00 00 04
AT_CERT_31d	EAC2_1.1	Compare DG4	80 06 00 00 00 00 00 00 08
AT_CERT_31e	EAC2_1.1	Compare DG5	80 06 00 00 00 00 00 00 10
AT_CERT_31f	EAC2_1.1	Compare DG6	80 06 00 00 00 00 00 00 20

Cert-ID	Version	Access Right	Authorization Extension
AT_CERT_31g	EAC2_1.1	Compare DG7	80 06 00 00 00 00 00 00 40
AT_CERT_31h	EAC2_1.1	Compare DG8	80 06 00 00 00 00 00 00 80
AT_CERT_31i	EAC2_1.1	Compare DG9	80 06 00 00 00 00 00 01 00
AT_CERT_31j	EAC2_1.1	Compare DG10	80 06 00 00 00 00 00 02 00
AT_CERT_31k	EAC2_1.1	Compare DG11	80 06 00 00 00 00 00 04 00
AT_CERT_31l	EAC2_1.1	Compare DG12	80 06 00 00 00 00 00 08 00
AT_CERT_31m	EAC2_1.1	Compare DG13	80 06 00 00 00 00 00 10 00
AT_CERT_31n	EAC2_1.1	Compare DG14	80 06 00 00 00 00 00 20 00
AT_CERT_31o	EAC2_1.1	Compare DG15	80 06 00 00 00 00 00 40 00
AT_CERT_31p	EAC2_1.1	Compare DG16	80 06 00 00 00 00 00 80 00
AT_CERT_31q	EAC2_1.1	Compare DG17	80 06 00 00 00 01 00 00
AT_CERT_31r	EAC2_1.1	Compare DG18	80 06 00 00 00 02 00 00
AT_CERT_31s	EAC2_1.1	Compare DG19	80 06 00 00 00 04 00 00
AT_CERT_31t	EAC2_1.1	Compare DG20	80 06 00 00 00 08 00 00
AT_CERT_31u	EAC2_1.1	Compare DG21	80 06 00 00 00 10 00 00
AT_CERT_31v	EAC2_1.1	Compare DG22	80 06 00 00 00 20 00 00
AT_CERT_31w	EAC2_1.1	No Compare	80 06 00 00 00 00 00 00 00

Table 6: Authorization Extension of AT_CERT_31

2.4.32 Certificate Set 32

The certificate set follows a certification scheme where RFU bits and unknown OIDs are used to verify the tolerance of eID cards concerning evolution of certificate extensions. Additionally, these certificates are used to verify that eID cards allow to activate and deactivate features by link certificates.

2.4.32.1 DV_CERT_32a

ID	DV CERT_32a
Purpose	This certificate is a non-official DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits access to a RFU eID function (bit 44, Read DG 23).
Version	EAC2_1.2
Referred by	Test case EAC2_ISO7816_L_38
Content definition	7F 21 aa 7F 4E bb

Test plan for eID-Cards with EAC 2.0

	<pre> 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 40 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 80 06 10 00 00 00 00 00 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>
Parameter	Certification Authority Reference
	As defined by the initial AT CVCA reference
	Certificate Holder Reference
	DETESTDVDE032
	Certificate Holder Authorization
	Non-official domestic DV, RFU bit 44 (Read DG 23)
	CVCA _{eff}
Parameter	Certificate effective date
	CVCA _{eff} + 1 month
Parameter	Certificate expiration date
	Public key of key pair DV KEY_32
Parameter	Public Key reference
	Signed with the private key of key pair CVCA_KEY_17

2.4.32.2 DV_CERT_32b

ID	DV_CERT_32b
Purpose	This certificate is a non-official DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits access to a RFU eID special function (bit 5, undefined).
Version	EAC2_1.2
Referred by	Test case EAC2_ISO7816_L_39
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 40

	<pre> 7F FF FF FF 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> 65 <i>kk</i> 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 80 01 20 5F 37 <i>ii jj</i> </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>
Parameter	Certification Authority Reference
	As defined by the initial AT CVCA reference
	Certificate Holder Reference
	DETTESTDVDE032
	Certificate Holder Authorization
	Non-official domestic DV, RFU bit 5
	Certificate effective date

2.4.32.3 DV_CERT_32c

ID	DV_CERT_32c
Purpose	This certificate is a non-official DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate contains a longer authorization extension for authentication terminals by two leading bytes ('00 00', 56 bits instead of 40 bits).
Version	EAC2_1.2
Referred by	Test case EAC2_ISO7816_L_40
Content definition	<pre> 7F 21 <i>aa</i> 7F 4E <i>bb</i> 5F 29 01 00 42 <i>cc dd</i> 7F 49 <i>ee ff</i> 5F 20 <i>xx yy</i> 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 07 00 00 40 7F FF FF FF 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> </pre>

	5F 37 ii jj aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate kk is the encoded length of the certificate extension object ll is the encoded length of the Discretionary Data Object ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)
Parameter	Certification Authority Reference
	As defined by the initial AT CVCA reference
	Certificate Holder Reference
	DETTESTDVDE032
	Certificate Holder Authorization
	Non-official domestic DV, Authorization Extension for Authentication Terminals extended by two bytes
	Certificate effective date

2.4.32.4 DV_CERT_32d

ID	DV_CERT_32d
Purpose	This certificate is a non-official DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate contains a longer authorization extension for eID access by two leading bytes ('00 00', 64 bits instead of 48 bits).
Version	EAC2_1.2
Referred by	Test case EAC2_ISO7816_L_41
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 40 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 80 08 00 00 00 00 00 00 00 01 5F 37 ii jj

	<p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (<i>cc</i> bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (<i>ee</i> bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (<i>xx</i> bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (<i>ii</i> bytes)</p>
Parameter	Certification Authority Reference
	As defined by the initial AT CVCA reference
	Certificate Holder Reference
	DETESTDVDE032
	Certificate Holder Authorization
	Non-official domestic DV, Authorization Extension for eID access extended by two bytes
	Certificate effective date

2.4.32.5 DV_CERT_32e

ID	DV CERT 32e
Purpose	This certificate is a non-official DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate contains a longer authorization extension for special functions by two leading bytes ('00 00', 24 bits instead of 8 bits).
Version	EAC2 1.2
Referred by	Test case EAC2_ISO7816_L_42
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 40 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 80 03 00 00 01 5F 37 ii jj </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object</p>

	cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate kk is the encoded length of the certificate extension object ll is the encoded length of the Discretionary Data Object ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)	
Parameter	Certification Authority Reference	As defined by the initial AT CVCA reference
	Certificate Holder Reference	DETTESTDVDE032
	Certificate Holder Authorization	Non-official domestic DV, Authorization Extension for special functions extended by two bytes
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_32
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17

2.4.32.6 DV_CERT_32f

ID	DV_CERT_32f
Purpose	This certificate is a non-official DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate contains an undefined OID (06 09 04 00 7F 00 07 03 01 02 03) in CHA for authentication terminals.
Version	EAC2 1.2
Referred by	Test case EAC2 ISO7816 L 43
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 03 53 05 40 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference</p>

	<p><i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	As defined by the initial AT CVCA reference
	Certificate Holder Reference	DETESTDVDE032
	Certificate Holder Authorization	Non-official domestic DV, Certificate Extension with unknown OID
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_32
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17

2.4.32.7 DV_CERT_32g

ID	DV_CERT_32g
Purpose	This certificate is a non-official DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate contains an undefined authorization extension OID (06 0A 04 00 7F 00 07 03 01 02 02 02) for eID access.
Version	EAC2_1.2
Referred by	Test case EAC2_ISO7816_L_44
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 40 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 02 02 80 06 00 00 00 00 00 01 5F 37 ii jj </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate</p>

	<p><i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	As defined by the initial AT CVCA reference
	Certificate Holder Reference	DETTESTDVDE032
	Certificate Holder Authorization	Non-official domestic DV, Authorization Extension for eID access with unknown OID
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair DV KEY 32
	Signing Key reference	Signed with the private key of key pair CVCA KEY 17

2.4.32.8 DV_CERT_32h

ID	DV_CERT_32h
Purpose	This certificate is a non-official DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate contains an unknown authorization extension OID for special functions (06 0A 04 00 7F 00 07 03 01 02 02 02).
Version	EAC2 1.2
Referred by	Test case EAC2 ISO7816 L 45
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 40 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 02 02 80 01 01 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>

Parameter	Certification Authority Reference	As defined by the initial AT CVCA reference
	Certificate Holder Reference	DETESTDVDE032
	Certificate Holder Authorization	Non-official domestic DV, Authorization Extension with unknown OID
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair DV KEY_32
	Signing Key reference	Signed with the private key of key pair CVCA KEY_17

2.4.32.9 AT_CERT_32a

ID	AT_CERT_32a						
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_32a. It encodes access rights for the RFU eID function “Read DG 23” in Authorization Extensions.						
Version	EAC2 1.2						
Referred by	Test case EAC2 ISO7816 L 38						
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 80 06 10 00 00 00 00 00 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>						
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTDVDE032</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTATDE032</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Terminal, Read DG 23 (RFU)</td> </tr> </table>	Certification Authority Reference	DETESTDVDE032	Certificate Holder Reference	DETESTATDE032	Certificate Holder Authorization	Terminal, Read DG 23 (RFU)
Certification Authority Reference	DETESTDVDE032						
Certificate Holder Reference	DETESTATDE032						
Certificate Holder Authorization	Terminal, Read DG 23 (RFU)						

	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair AT_KEY_32
	Signing Key reference	Signed with the private key of key pair DV_KEY_32

2.4.32.10 AT_CERT_32b

ID	AT_CERT_32b														
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_32b. It encodes access rights for an RFU eID special function in Authorization Extensions.														
Version	EAC2_1.2														
Referred by	Test case EAC2 ISO7816 L_39														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 80 01 20 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTDVDE032</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTSTATDE032</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Terminal, RFU bit 5</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair AT_KEY_32</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair DV_KEY_32</td> </tr> </table>	Certification Authority Reference	DETESTDVDE032	Certificate Holder Reference	DETESTSTATDE032	Certificate Holder Authorization	Terminal, RFU bit 5	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair AT_KEY_32	Signing Key reference	Signed with the private key of key pair DV_KEY_32
Certification Authority Reference	DETESTDVDE032														
Certificate Holder Reference	DETESTSTATDE032														
Certificate Holder Authorization	Terminal, RFU bit 5														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair AT_KEY_32														
Signing Key reference	Signed with the private key of key pair DV_KEY_32														

2.4.32.11 AT_CERT_32c

ID	AT_CERT_32c															
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_32c. The certificate contains a longer authorization extension for authentication terminals by two leading bytes ('00 00', 56 bits instead of 40 bits).															
Version	EAC2_1.2															
Referred by	Test case EAC2_ISO7816_L_40															
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 07 00 00 00 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>															
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTDVDE032</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTATDE032</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Terminal, Authorization Extension for Authentication Terminals extended by two bytes</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair AT_KEY_32</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair DV_KEY_32</td> </tr> </table>		Certification Authority Reference	DETESTDVDE032	Certificate Holder Reference	DETESTATDE032	Certificate Holder Authorization	Terminal, Authorization Extension for Authentication Terminals extended by two bytes	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair AT_KEY_32	Signing Key reference	Signed with the private key of key pair DV_KEY_32
Certification Authority Reference	DETESTDVDE032															
Certificate Holder Reference	DETESTATDE032															
Certificate Holder Authorization	Terminal, Authorization Extension for Authentication Terminals extended by two bytes															
Certificate effective date	CVCA _{eff}															
Certificate expiration date	CVCA _{eff} + 1 month															
Public Key reference	Public key of key pair AT_KEY_32															
Signing Key reference	Signed with the private key of key pair DV_KEY_32															

2.4.32.12 AT_CERT_32d

ID	AT_CERT_32d
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_32d. The certificate contains a longer authorization extension for eID functions by two leading bytes ('00 00', 64 bits instead of 48 bits).

Test plan for eID-Cards with EAC 2.0

Version	EAC2_1.2														
Referred by	Test case EAC2_ISO7816_L_41														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 80 08 00 00 00 00 00 00 00 01 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETTESTDVDE032</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETTESTATDE032</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Terminal, Authorization Extension for eID functions extended by two bytes</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair AT_KEY_32</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair DV_KEY_32</td> </tr> </table>	Certification Authority Reference	DETTESTDVDE032	Certificate Holder Reference	DETTESTATDE032	Certificate Holder Authorization	Terminal, Authorization Extension for eID functions extended by two bytes	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair AT_KEY_32	Signing Key reference	Signed with the private key of key pair DV_KEY_32
Certification Authority Reference	DETTESTDVDE032														
Certificate Holder Reference	DETTESTATDE032														
Certificate Holder Authorization	Terminal, Authorization Extension for eID functions extended by two bytes														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair AT_KEY_32														
Signing Key reference	Signed with the private key of key pair DV_KEY_32														

2.4.32.13 AT_CERT_32e

ID	AT_CERT_32e
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_32e. The certificate contains a longer authorization extension for special functions by two leading bytes ('00 00', 24 bits instead of 8 bits).
Version	EAC2_1.2
Referred by	Test case EAC2_ISO7816_L_42
Content definition	7F 21 aa

	<pre> 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 80 03 00 00 01 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>
Parameter	Certification Authority Reference
	DETESTDVDE032
	Certificate Holder Reference
	DETESTATDE032
	Certificate Holder Authorization
	Terminal, Authorization Extension for special functions extended by two bytes
	Certificate effective date
	CVCA _{eff}
	Certificate expiration date
	CVCA _{eff} + 1 month
	Public Key reference
	Public key of key pair AT_KEY_32
	Signing Key reference
	Signed with the private key of key pair DV_KEY_32

2.4.32.14 AT_CERT_32f

ID	AT_CERT_32f
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_32f. The certificate contains an unknown OID in CHA.
Version	EAC2 1.2
Referred by	Test case EAC2_ISO7816_L_43
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 03 53 05 00 7F FF

	FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)
Parameter	Certification Authority Reference
	DETESTDVDE032
	Certificate Holder Reference
	DETESTATDE032
	Certificate Holder Authorization
	Terminal, Certificate Extension with unknown OID
	CVCA _{eff}

2.4.32.15 AT_CERT_32g

ID	AT_CERT_32g
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_32g. The certificate contains an unknown authorization extension OID for eID access.
Version	EAC2_1.2
Referred by	Test case EAC2_ISO7816_L_44
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 02 80 06 00 00 00 00 00 01 5F 37 ii jj <i>aa</i> is the encoded combined length of certificate body and signature objects

	<p><i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>kk</i> is the encoded length of the certificate extension object <i>ll</i> is the encoded length of the Discretionary Data Object <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	DETESTDVDE032
	Certificate Holder Reference	DETESTATDE032
	Certificate Holder Authorization	Terminal, Authorization Extension fwith unknown OID
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair AT_KEY_32
	Signing Key reference	Signed with the private key of key pair DV_KEY_32

2.4.32.16 AT_CERT_32h

ID	AT_CERT_32h
Purpose	This certificate is a regular terminal certificate, which is issued by the DV_CERT_32h. The certificate contains an unknown authorization extension OID for special functions.
Version	EAC2_1.2
Referred by	Test case EAC2_ISO7816_L_45
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 00 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 02 80 01 01 5F 37 ii jj </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference</p>

	yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate kk is the encoded length of the certificate extension object ll is the encoded length of the Discretionary Data Object ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)	
Parameter	Certification Authority Reference	DETTESTDVDE032
	Certificate Holder Reference	DETTESTATDE032
	Certificate Holder Authorization	Terminal, Authorization Extension with unknown OID
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair AT_KEY_32
	Signing Key reference	Signed with the private key of key pair DV_KEY_32

2.4.32.17 LINK_CERT_32a

ID	LINK_CERT_32a
Purpose	This certificate is a link certificate, which activates the access right to read eID data group 1.
Version	EAC2_1.2
Referred by	Test case EAC2_ISO7816_M_9. Test case EAC2_ISO7816_M_10, Test case EAC2_ISO7816_M_11
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 C0 00 00 01 00 5F 25 06 gg 5F 24 06 hh optional: 65 vv ww 5F 37 ii jj <p>aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes) vv is the encoded length of the certificate extension,</p>

	ww is the placeholder for the certificate extension (vv bytes)	
Parameter	Certification Authority Reference	As defined by the initial AT CVCA reference
	Certificate Holder Reference	DETESTLINKDE32A
	Certificate Holder Authorization	CVCA, read access to EID_DG 1
	Certificate effective date	CVCA _{exp} + 5 month - 1 day
	Certificate expiration date	CVCA _{exp} + 8 month
	Public Key reference	Public key of key pair AT_CVCA_KEY_32
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
	Certificate Extension	As defined by CVCA

2.4.32.18 LINK_CERT_32b

ID	LINK_CERT_32b	
Purpose	This certificate is a link certificate, which deactivates the access right to read eID data group 1.	
Version	EAC2_1.2	
Referred by	Test case EAC2_ISO7816_M_9, Test case EAC2_ISO7816_M_10, Test case EAC2_ISO7816_M_11	
Content definition	<p> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 C0 00 00 00 00 5F 25 06 gg 5F 24 06 hh optional: 65 vv ww 5F 37 ii jj </p> <p> aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes) vv is the encoded length of the certificate extension, ww is the placeholder for the certificate extension (vv bytes) </p>	
Parameter	Certification Authority Reference	As defined by the initial AT CVCA reference
	Certificate Holder Reference	DETESTLINKDE32B

Certificate Holder Authorization	CVCA, no rights
Certificate effective date	CVCA _{exp} + 5 month - 1 day
Certificate expiration date	CVCA _{exp} + 8 month
Public Key reference	Public key of key pair AT_CVCA_KEY_32
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
Certificate Extension	As defined by CVCA

2.4.32.19 LINK_CERT_32c

ID	LINK_CERT_32c								
Purpose	This certificate is a link certificate, which activates the access right to compare eID data group 8 (date of birth).								
Version	EAC2 1.2								
Referred by	Test case EAC2_ISO7816_M_12. Test case EAC2_ISO7816_M_13, Test case EAC2_ISO7816_M_14								
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 C0 00 00 80 00 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 80 06 00 00 00 00 00 80 5F 37 ii jj</p> <p>aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes) vv is the encoded length of the certificate extension, ww is the placeholder for the certificate extension (vv bytes)</p>								
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the initial AT CVCA reference</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTLINKDE32C</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>CVCA, read access to EID_DG 1, compare DG 1</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{exp} + 5 month - 1 day</td> </tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTLINKDE32C	Certificate Holder Authorization	CVCA, read access to EID_DG 1, compare DG 1	Certificate effective date	CVCA _{exp} + 5 month - 1 day
Certification Authority Reference	As defined by the initial AT CVCA reference								
Certificate Holder Reference	DETESTLINKDE32C								
Certificate Holder Authorization	CVCA, read access to EID_DG 1, compare DG 1								
Certificate effective date	CVCA _{exp} + 5 month - 1 day								

Certificate expiration date	CVCA _{exp} + 8 month
Public Key reference	Public key of key pair AT_CVCA_KEY_32
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
Certificate Extension	As defined by CVCA

2.4.32.20 LINK_CERT_32d

ID	LINK CERT 32d												
Purpose	This certificate is a link certificate, which deactivates the access right to compare eID data group 8 (date of birth).												
Version	EAC2 1.2												
Referred by	Test case EAC2_ISO7816_M_12. Test case EAC2_ISO7816_M_13, Test case EAC2_ISO7816_M_14												
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 C0 00 00 00 00 5F 25 06 gg 5F 24 06 hh 65 kk 73 11 06 0A 04 00 7F 00 07 03 01 02 02 01 80 06 00 00 00 00 00 00 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) <i>vv</i> is the encoded length of the certificate extension, <i>ww</i> is the placeholder for the certificate extension (vv bytes)</p>												
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the initial AT CVCA reference</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTLINKDE32D</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>CVCA, no rights</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{exp} + 5 month - 1 day</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{exp} + 8 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair AT_CVCA_KEY_32</td> </tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTLINKDE32D	Certificate Holder Authorization	CVCA, no rights	Certificate effective date	CVCA _{exp} + 5 month - 1 day	Certificate expiration date	CVCA _{exp} + 8 month	Public Key reference	Public key of key pair AT_CVCA_KEY_32
Certification Authority Reference	As defined by the initial AT CVCA reference												
Certificate Holder Reference	DETESTLINKDE32D												
Certificate Holder Authorization	CVCA, no rights												
Certificate effective date	CVCA _{exp} + 5 month - 1 day												
Certificate expiration date	CVCA _{exp} + 8 month												
Public Key reference	Public key of key pair AT_CVCA_KEY_32												

	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
	Certificate Extension	As defined by CVCA

2.4.33 Certificate Set 33

This certificate set consists of a regular certificate chain (DV → AT) which is used for the tests regarding AT. The DV certificate permits read access to all elementary files. The DV certificate is an official domestic certificate.

2.4.33.1 DV_CERT_33

ID	DV_CERT_33												
Purpose	This certificate is a regular DV certificate, which validity period starts at the effective date of the CVCA and expires after one month. The certificate permits read access to all elementary files												
Version	Smart-eID												
Referred by													
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 3F FF FF 10 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>												
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the initial AT CVCA reference</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETTESTDVDE033</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Official domestic DV, Read Access (all)</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_33</td> </tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETTESTDVDE033	Certificate Holder Authorization	Official domestic DV, Read Access (all)	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_33
Certification Authority Reference	As defined by the initial AT CVCA reference												
Certificate Holder Reference	DETTESTDVDE033												
Certificate Holder Authorization	Official domestic DV, Read Access (all)												
Certificate effective date	CVCA _{eff}												
Certificate expiration date	CVCA _{eff} + 1 month												
Public Key reference	Public key of key pair DV_KEY_33												

	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33
--	-----------------------	--

2.4.33.2 DV_CERT_33a

ID	DV_CERT_33a	
Purpose	This certificate is similar to DV_Cert_33, but does not contain a Certificate Holder Authorization	
Version	Smart-eID	
Referred by	Test case EAC2_ISO7816_J_6	
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	As defined by the initial AT CVCA reference
	Certificate Holder Reference	DETESTDVDE033
	Certificate Holder Authorization	absent
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_33
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17

2.4.33.3 DV_CERT_33b

ID	DV_CERT_33b
Purpose	This certificate is similar to DV_Cert_33, but does not contain a Certificate Effective Date
Version	Smart-eID

Test plan for eID-Cards with EAC 2.0

Referred by	Test case EAC2_ISO7816_J_7														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 3F FF FF 10 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the initial AT CVCA reference</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE033</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Official domestic DV, Read Access (all)</td> </tr> <tr> <td>Certificate effective date</td> <td>absent</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_33</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_17</td> </tr> </table>	Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTDVDE033	Certificate Holder Authorization	Official domestic DV, Read Access (all)	Certificate effective date	absent	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_33	Signing Key reference	Signed with the private key of key pair CVCA_KEY_17
Certification Authority Reference	As defined by the initial AT CVCA reference														
Certificate Holder Reference	DETESTDVDE033														
Certificate Holder Authorization	Official domestic DV, Read Access (all)														
Certificate effective date	absent														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_33														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_17														

2.4.33.4 DV_CERT_33c

ID	DV_CERT_33c
Purpose	This certificate is similar to DV_Cert_33, but does not contain a Certificate Expiration Date
Version	Smart-eID
Referred by	Test case EAC2_ISO7816_J8
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 3F FF FF 10 5F 25 06 gg 5F 37 ii jj</p>

	<p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	As defined by the initial AT CVCA reference
	Certificate Holder Reference	DETESTDVDE033
	Certificate Holder Authorization	Official domestic DV, Read Access (all)
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	absent
	Public Key reference	Public key of key pair DV_KEY_33
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33

2.4.33.5 DV_CERT_33d

ID	DV_CERT_33d
Purpose	This certificate is similar to DV_Cert_33, but contains a badly encoded Certificate Effective Date (invalid BCD encoding)
Version	Smart-eID
Referred by	Test case EAC2_ISO7816_J_9
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 3F FF FF 10 5F 25 06 0A 0B 0C 0D 0E 0F 5F 24 06 hh 5F 37 ii jj </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate</p>

	<i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (<i>ii</i> bytes)	
Parameter	Certification Authority Reference	As defined by the initial AT CVCA reference
	Certificate Holder Reference	DETESTDVDE033
	Certificate Holder Authorization	Official domestic DV, Read Access (all)
	Certificate effective date	0A 0B 0C 0D 0E 0F (invalid BCD encoding)
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair DV KEY_33
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33

2.4.33.6 DV_CERT_33e

ID	DV_CERT_33e	
Purpose	This certificate is similar to DV_Cert_33, but contains a badly encoded Certificate Expiration Date (invalid BCD encoding)	
Version	Smart-eID	
Referred by	Test case EAC2 ISO7816 J 10	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 3F FF FF 10 5F 25 06 gg 5F 24 06 0A 0B 0C 0D 0E 0F 5F 37 ii jj <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (<i>cc</i> bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (<i>ee</i> bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (<i>xx</i> bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (<i>ii</i> bytes)</p>	
Parameter	Certification Authority Reference Certificate Holder Reference Certificate Holder Authorization Certificate effective date Certificate expiration date	

	Public Key reference	Public key of key pair DV_KEY_33
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33

2.4.33.7 DV_CERT_33f

ID	DV_CERT_33f															
Purpose	This certificate is similar to DV_Cert_33, but contains a badly encoded Certificate Effective Date (invalid BCD encoding)															
Version	Smart-eID															
Referred by	Test case EAC2_ISO7816_J_17															
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 3F FF FF 10 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>															
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the initial AT CVCA reference</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE033</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Official domestic DV, Read Access (all)</td> </tr> <tr> <td>Certificate effective date</td> <td>The month and the year used as defined by the CVCA_{eff} and the day is always set to the 32nd so that it becomes an invalid Gregorian date.</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_33</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_33</td> </tr> </table>		Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTDVDE033	Certificate Holder Authorization	Official domestic DV, Read Access (all)	Certificate effective date	The month and the year used as defined by the CVCA _{eff} and the day is always set to the 32 nd so that it becomes an invalid Gregorian date.	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_33	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33
Certification Authority Reference	As defined by the initial AT CVCA reference															
Certificate Holder Reference	DETESTDVDE033															
Certificate Holder Authorization	Official domestic DV, Read Access (all)															
Certificate effective date	The month and the year used as defined by the CVCA _{eff} and the day is always set to the 32 nd so that it becomes an invalid Gregorian date.															
Certificate expiration date	CVCA _{eff} + 1 month															
Public Key reference	Public key of key pair DV_KEY_33															
Signing Key reference	Signed with the private key of key pair CVCA_KEY_33															

2.4.33.8 DV_CERT_33g

ID	DV_CERT_33g															
Purpose	This certificate is similar to DV_Cert_33, but contains a badly encoded Certificate Effective Date (invalid BCD encoding)															
Version	Smart-eID															
Referred by	Test case EAC_ISO7816_J_18															
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 3F FF FF 10 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>															
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the initial AT CVCA reference</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE033</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Official domestic DV, Read Access (all)</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>The month and the year used as defined by the CVCA_{eff} and the day is always set to the 32nd so that it becomes an invalid Gregorian date.</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_33</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_33</td> </tr> </table>		Certification Authority Reference	As defined by the initial AT CVCA reference	Certificate Holder Reference	DETESTDVDE033	Certificate Holder Authorization	Official domestic DV, Read Access (all)	Certificate effective date	CVCA _{eff}	Certificate expiration date	The month and the year used as defined by the CVCA _{eff} and the day is always set to the 32 nd so that it becomes an invalid Gregorian date.	Public Key reference	Public key of key pair DV_KEY_33	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33
Certification Authority Reference	As defined by the initial AT CVCA reference															
Certificate Holder Reference	DETESTDVDE033															
Certificate Holder Authorization	Official domestic DV, Read Access (all)															
Certificate effective date	CVCA _{eff}															
Certificate expiration date	The month and the year used as defined by the CVCA _{eff} and the day is always set to the 32 nd so that it becomes an invalid Gregorian date.															
Public Key reference	Public key of key pair DV_KEY_33															
Signing Key reference	Signed with the private key of key pair CVCA_KEY_33															

2.4.33.9 DV_CERT_33h

ID	DV_CERT_33h
Purpose	This certificate is similar to DV_Cert_33, but contains a Certificate Expiration Date BEFORE the Certificate Effective Date
Version	Smart-eID
Referred by	Test case EAC2_ISO7816_J_19

Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 3F FF FF 10 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>
Parameter	Certification Authority Reference
	As defined by the initial AT CVCA reference
	Certificate Holder Reference
	DETESTDVDE033
	Certificate Holder Authorization
	Official domestic DV, Read Access (all)
	Certificate effective date

2.4.33.10 DV_CERT_33i

ID	DV_CERT_33i
Purpose	This certificate is similar to DV_CERT_33, but contains a Certificate Holder Authorization with an invalid combination of OID (<id-AT>) and discretionary data object (structured like a relative authorization bit map for an IS)
Version	Smart-eID
Referred by	Test case EAC2_ISO7816_J_21
Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 3F FF FF 10</pre>

	<p style="text-align: center;"> 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </p> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>
Parameter	Certification Authority Reference
	As defined by the initial AT CVCA reference
	Certificate Holder Reference
	DETESTDVDE033
	Certificate Holder Authorization
	Domestic DV, access to ePassport DG3 and DG4
	Certificate effective date

2.4.33.11 DV_CERT_33j

ID	DV_CERT_33j
Purpose	This certificate is similar to DV_CERT_33, but contains a Public Key with an invalid OID
Version	Smart-eID
Referred by	Test case EAC2_ISO7816_J_22
Content definition	<p style="text-align: center;"> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 02 53 05 80 3F FF FF 10 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </p> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), </p>

	xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)	
Parameter	Certification Authority Reference	As defined by the initial AT CVCA reference
	Certificate Holder Reference	DETTESTDVDE033
	Certificate Public Key	Invalid OID (Use 0.4.0.127.0.7.2.2.5.1)
	Certificate Holder Authorization	Official domestic DV, Read Access (all)
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 1 month
	Public Key reference	Public key of key pair DV_KEY_33
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33

2.4.33.12 DV_CERT_33k

ID	DV_CERT_33k	
Purpose	This certificate is similar to DV_CERT_33, but contains longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.	
Version	Smart-eID	
Referred by	Test case EAC2 ISO7816 J 23, Test case EAC2 ISO7816 J 33	
Content definition	7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj <p>aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes), xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object, jj is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	As defined by the CVCA

Certificate Holder Reference	DETTESTDVDE033
Certificate Holder Authorization	Official domestic DV, Read Access (all)
Certificate effective date	CVCA _{eff} + 1 month + 20 days
Certificate expiration date	CVCA _{eff} + 1 month + 25 days
Public Key reference	Public key of key pair DV_KEY_33
Signing Key reference	Signed with the private key of key pair CVCA_KEY_33

2.4.33.13 DV_CERT_33I

ID	DV_CERT_33I	
Purpose	This certificate is similar to DV_CERT_33, but contains a wrong tag for certificate body and longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.	
Version	Smart-eID	
Referred by	Test case EAC2 ISO7816 J 24	
Content definition	7F 21 aa 7F 4F bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference As defined by the CVCA Certificate Holder Reference DETTESTDVDE033 Certificate Holder Authorization Official domestic DV, Read Access (all) Certificate effective date CVCA _{eff} + 1 month + 20 days Certificate expiration date CVCA _{eff} + 1 month + 25 days Public Key reference Public key of key pair DV_KEY_33 Signing Key reference Signed with the private key of key pair CVCA_KEY_33	

2.4.33.14 DV_CERT_33m

ID	DV_CERT_33m															
Purpose	This certificate is similar to DV_CERT_33, but contains a wrong tag for certificate signature and longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.															
Version	Smart-eID															
Referred by	Test case EAC2_ISO7816_J_25															
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 38 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>															
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE033</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Official domestic DV, Read Access (all)</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff} + 1 month + 20 days</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month + 25 days</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_33</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_33</td> </tr> </table>		Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE033	Certificate Holder Authorization	Official domestic DV, Read Access (all)	Certificate effective date	CVCA _{eff} + 1 month + 20 days	Certificate expiration date	CVCA _{eff} + 1 month + 25 days	Public Key reference	Public key of key pair DV_KEY_33	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33
Certification Authority Reference	As defined by the CVCA															
Certificate Holder Reference	DETESTDVDE033															
Certificate Holder Authorization	Official domestic DV, Read Access (all)															
Certificate effective date	CVCA _{eff} + 1 month + 20 days															
Certificate expiration date	CVCA _{eff} + 1 month + 25 days															
Public Key reference	Public key of key pair DV_KEY_33															
Signing Key reference	Signed with the private key of key pair CVCA_KEY_33															

2.4.33.15 DV_CERT_33n

ID	DV_CERT_33n
Purpose	This certificate is similar to DV_CERT_33, but contains a wrong certificate body length and longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.
Version	Smart-eID
Referred by	Test case EAC2_ISO7816_J_26

Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object decreased by one <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>
Parameter	Certification Authority Reference
	As defined by the CVCA
	Certificate Holder Reference
	DETESTDVDE033
	Certificate Holder Authorization
	Official domestic DV, Read Access (all)
	Certificate effective date

2.4.33.16 DV_CERT_33o

ID	DV_CERT_33o
Purpose	This certificate is similar to DV_CERT_33, but contains a wrong certificate signature length and longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.
Version	Smart-eID
Referred by	Test case EAC2_ISO7816_J_27
Content definition	<pre>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg</pre>

	<p style="text-align: center;">5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object decreased by one <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>
Parameter	Certification Authority Reference
	As defined by the CVCA
	Certificate Holder Reference
	DETESTDVDE033
	Certificate Holder Authorization
	Official domestic DV, Read Access (all)
	Certificate effective date
	CVCA _{eff} + 1 month + 20 days
	Certificate expiration date
	CVCA _{eff} + 1 month + 25 days
	Public Key reference
	Public key of key pair DV KEY_33
	Signing Key reference
	Signed with the private key of key pair CVCA KEY_33

2.4.33.17 DV_CERT_33p

ID	DV_CERT_33p
Purpose	This certificate is similar to DV_CERT_33, but contains a wrong certificate signature and longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.
Version	Smart-eID
Referred by	Test case EAC2_ISO7816_J_28
Content definition	<p style="text-align: center;">7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key,</p>

	<code>ff</code> is the placeholder for the certificate's public key bytes (ee bytes), <code>xx</code> is the encoded length of the Certificate Holder Reference <code>yy</code> is the placeholder for the Certificate Holder Reference (xx bytes) <code>gg</code> is the placeholder for the BCD encoded effective date of the certificate <code>hh</code> is the placeholder for the BCD encoded expiration date of the certificate <code>ii</code> is the encoded length of the certificates signature object <code>jj</code> is the placeholder for the certificates signature (ii bytes) last byte is increased by one (mod 256)	
Parameter	Certification Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETTESTDVDE033
	Certificate Holder Authorization	Official domestic DV, Read Access (all)
	Certificate effective date	CVCA _{eff} + 1 month + 20 days
	Certificate expiration date	CVCA _{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_33
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33

2.4.33.18 DV_CERT_33q

ID	DV_CERT_33q
Purpose	This certificate is similar to DV_CERT_33, but contains a wrong certificate signature and longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.
Version	Smart-eID
Referred by	Test case EAC2 ISO7816 J 29
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <code>aa</code> is the encoded combined length of certificate body and signature objects <code>bb</code> is the encoded length of the certificate body object <code>cc</code> is the encoded length of the Certification Authority Reference <code>dd</code> is the placeholder for the Certification Authority Reference (cc bytes) <code>ee</code> is the encoded length of the certificate's public key, <code>ff</code> is the placeholder for the certificate's public key bytes (ee bytes), <code>xx</code> is the encoded length of the Certificate Holder Reference <code>yy</code> is the placeholder for the Certificate Holder Reference (xx bytes) <code>gg</code> is the placeholder for the BCD encoded effective date of the certificate <code>hh</code> is the placeholder for the BCD encoded expiration date of the certificate <code>ii</code> is the encoded length of the certificates signature object <code>jj</code> is the placeholder for the certificates signature (ii bytes) – last byte is dropped and ii is </p>

updated according to the new length		
Parameter	Certification Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE033
	Certificate Holder Authorization	Official domestic DV, Read Access (all)
	Certificate effective date	CVCA _{eff} + 1 month + 20 days
	Certificate expiration date	CVCA _{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_33
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33

2.4.33.19 DV_CERT_33r

ID	DV_CERT_33r										
Purpose	This certificate is similar to DV_CERT_33, but contains a wrong certificate public key and longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.										
Version	Smart-eID										
Referred by	Test case EAC2 ISO7816 J 35										
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p>aa is the encoded combined length of certificate body and signature objects bb is the encoded length of the certificate body object cc is the encoded length of the Certification Authority Reference dd is the placeholder for the Certification Authority Reference (cc bytes) ee is the encoded length of the certificate's public key, ff is the placeholder for the certificate's public key bytes (ee bytes) – it does not contain any OID DO, xx is the encoded length of the Certificate Holder Reference yy is the placeholder for the Certificate Holder Reference (xx bytes) gg is the placeholder for the BCD encoded effective date of the certificate hh is the placeholder for the BCD encoded expiration date of the certificate ii is the encoded length of the certificates signature object jj is the placeholder for the certificates signature (ii bytes)</p>										
Parameter	<table border="1"> <tbody> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE033</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Official domestic DV, Read Access (all)</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff} + 1 month + 20 days</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month + 25 days</td> </tr> </tbody> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE033	Certificate Holder Authorization	Official domestic DV, Read Access (all)	Certificate effective date	CVCA _{eff} + 1 month + 20 days	Certificate expiration date	CVCA _{eff} + 1 month + 25 days
Certification Authority Reference	As defined by the CVCA										
Certificate Holder Reference	DETESTDVDE033										
Certificate Holder Authorization	Official domestic DV, Read Access (all)										
Certificate effective date	CVCA _{eff} + 1 month + 20 days										
Certificate expiration date	CVCA _{eff} + 1 month + 25 days										

	Public Key reference	Public key of key pair DV_KEY_33
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33

2.4.33.20 DV_CERT_33s

ID	DV_CERT_33s														
Purpose	This certificate is similar to DV_CERT_33, but contains a wrong certificate public key and longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.														
Version	Smart-eID														
Referred by	Test case EAC2_ISO7816_J_34														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes) – the OID has an incorrect value that does not indicate id-TA: (0.4.0.127.0.7.2.2.3.x.y), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE033</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Official domestic DV, Read Access (all)</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff} + 1 month + 20 days</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month + 25 days</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_33</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_33</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE033	Certificate Holder Authorization	Official domestic DV, Read Access (all)	Certificate effective date	CVCA _{eff} + 1 month + 20 days	Certificate expiration date	CVCA _{eff} + 1 month + 25 days	Public Key reference	Public key of key pair DV_KEY_33	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETESTDVDE033														
Certificate Holder Authorization	Official domestic DV, Read Access (all)														
Certificate effective date	CVCA _{eff} + 1 month + 20 days														
Certificate expiration date	CVCA _{eff} + 1 month + 25 days														
Public Key reference	Public key of key pair DV_KEY_33														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_33														

2.4.33.21 DV_CERT_33t

ID	DV_CERT_33t														
Purpose	This certificate is similar to DV_CERT_33, but contains an invalid public key (ECDSA: wrong point on curve) and longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.														
Version	Smart-eID														
Referred by	Test case EAC2 ISO7816 J 36														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes) – the elliptic curve public point is missing, <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE033</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Official domestic DV, Read Access (all)</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff} + 1 month + 20 days</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month + 25 days</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_33</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_33</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE033	Certificate Holder Authorization	Official domestic DV, Read Access (all)	Certificate effective date	CVCA _{eff} + 1 month + 20 days	Certificate expiration date	CVCA _{eff} + 1 month + 25 days	Public Key reference	Public key of key pair DV_KEY_33	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETESTDVDE033														
Certificate Holder Authorization	Official domestic DV, Read Access (all)														
Certificate effective date	CVCA _{eff} + 1 month + 20 days														
Certificate expiration date	CVCA _{eff} + 1 month + 25 days														
Public Key reference	Public key of key pair DV_KEY_33														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_33														

2.4.33.22 DV_CERT_33u

ID	DV_CERT_33u
Purpose	This certificate is similar to DV_CERT_33, but contains an invalid public key (RSA: modulus is missing) and longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.
Version	Smart-eID

Test plan for eID-Cards with EAC 2.0

Referred by	Test case EAC2_ISO7816_J_37														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes) – the RSA modulus is missing, <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETTESTDVDE033</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Official domestic DV, Read Access (all)</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff} + 1 month + 20 days</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month + 25 days</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_33</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_33</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETTESTDVDE033	Certificate Holder Authorization	Official domestic DV, Read Access (all)	Certificate effective date	CVCA _{eff} + 1 month + 20 days	Certificate expiration date	CVCA _{eff} + 1 month + 25 days	Public Key reference	Public key of key pair DV_KEY_33	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETTESTDVDE033														
Certificate Holder Authorization	Official domestic DV, Read Access (all)														
Certificate effective date	CVCA _{eff} + 1 month + 20 days														
Certificate expiration date	CVCA _{eff} + 1 month + 25 days														
Public Key reference	Public key of key pair DV_KEY_33														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_33														

2.4.33.23 DV_CERT_33v

ID	DV_CERT_33v
Purpose	This certificate is similar to DV_CERT_33, but contains an invalid public key (RSA: exponent is missing) and longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.
Version	Smart-eID
Referred by	Test case EAC2_ISO7816_J_38
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff</p>

	<pre> 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <code>aa</code> is the encoded combined length of certificate body and signature objects <code>bb</code> is the encoded length of the certificate body object <code>cc</code> is the encoded length of the Certification Authority Reference <code>dd</code> is the placeholder for the Certification Authority Reference (cc bytes) <code>ee</code> is the encoded length of the certificate's public key, <code>ff</code> is the placeholder for the certificate's public key bytes (ee bytes) – the RSA public exponent is missing, <code>xx</code> is the encoded length of the Certificate Holder Reference <code>yy</code> is the placeholder for the Certificate Holder Reference (xx bytes) <code>gg</code> is the placeholder for the BCD encoded effective date of the certificate <code>hh</code> is the placeholder for the BCD encoded expiration date of the certificate <code>ii</code> is the encoded length of the certificates signature object <code>jj</code> is the placeholder for the certificates signature (ii bytes) </p>
Parameter	Certification Authority Reference
	As defined by the CVCA
	Certificate Holder Reference
	DETTESTDVDE033
	Certificate Holder Authorization
	Official domestic DV, Read Access (all)
	Certificate effective date
	CVCA _{eff} + 1 month + 20 days
	Certificate expiration date
	CVCA _{eff} + 1 month + 25 days
	Public Key reference
	Public key of key pair DV_KEY_33
	Signing Key reference
	Signed with the private key of key pair CVCA_KEY_33

2.4.33.24 DV_CERT_33w

ID	DV_CERT_33w
Purpose	This certificate is similar to DV_CERT_33, but contains an invalid public key: RSA: an unknown DO is present within the RSA parameters ('77 01 00') ECDSA: an unknown DO is present within the EC parameters (tag '77') Additionally, longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.
Version	Smart-eID
Referred by	Test case EAC2_ISO7816_J_39
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh </pre>

	<p>5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes) – an unknown DO '77 is present, <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>
Parameter	Certification Authority Reference
	As defined by the CVCA
	Certificate Holder Reference
	DETESTDVDE033
	Certificate Holder Authorization
	Official domestic DV, Read Access (all)
	Certificate effective date

2.4.33.25 DV_CERT_33x

ID	DV_CERT_33x
Purpose	This certificate is similar to DV_CERT_33, but contains a wrong certificate signature (RSA: sig = modulus + 1 or EC: sig = order + 1). Additionally, longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.
Version	Smart-eID
Referred by	Test case EAC2_ISO7816_J_30
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes)</p>

	<p><i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (<i>ee</i> bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (<i>xx</i> bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object <i>jj</i> is the placeholder for the certificates signature (<i>ii</i> bytes) – the signature is greater than the modulus of the issuing key CVCA_KEY_00, the length of signature matches the length of the modulus</p>	
Parameter	Certification Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETESTDVDE033
	Certificate Holder Authorization	Official domestic DV, Read Access (all)
	Certificate effective date	CVCA _{eff} + 1 month + 20 days
	Certificate expiration date	CVCA _{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV_KEY_33
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33

2.4.33.26 DV_CERT_33y

ID	DV_CERT_33y
Purpose	This certificate is similar to DV_CERT_33, but contains a wrong certificate signature (ECDSA). It is obtained by filling the ‘r’ part of the signature with ‘00’. The length of ‘r’ is still matches the size of the prime. Additionally, longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.
Version	Smart-eID
Referred by	Test cases EAC2_ISO7816_J_31
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (<i>cc</i> bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (<i>ee</i> bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (<i>xx</i> bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate</p>

	<p><i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object <i>jj</i> is the placeholder for the certificates signature (ii bytes) – with r=0</p>	
Parameter	Certification Authority Reference	As defined by the CVCA
	Certificate Holder Reference	DETTESTDVDE033
	Certificate Holder Authorization	Official domestic DV, Read Access (all)
	Certificate effective date	CVCA _{eff} + 1 month + 20 days
	Certificate expiration date	CVCA _{eff} + 1 month + 25 days
	Public Key reference	Public key of key pair DV KEY_33
	Signing Key reference	Signed with the private key of key pair CVCA_KEY_33

2.4.33.27 DV_CERT_33z

ID	DV_CERT_33z							
Purpose	<p>This certificate is similar to DV_CERT_33, but contains a wrong certificate signature (ECDSA). It is obtained by filling the ‘s’ part of the signature with ‘00’. The length of ‘s’ is still matches the size of the prime. Additionally, longer time spans for effective date and expiration date to detect malfunctioning chips indirectly.</p>							
Version	Smart-eID							
Referred by	Test cases EAC2 ISO7816 J 32							
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object <i>jj</i> is the placeholder for the certificates signature (ii bytes) – with s=0</p>							
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETTESTDVDE033</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Official domestic DV, Read Access (all)</td> </tr> </table>		Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETTESTDVDE033	Certificate Holder Authorization	Official domestic DV, Read Access (all)
Certification Authority Reference	As defined by the CVCA							
Certificate Holder Reference	DETTESTDVDE033							
Certificate Holder Authorization	Official domestic DV, Read Access (all)							

Certificate effective date	CVCA _{eff} + 1 month + 20 days
Certificate expiration date	CVCA _{eff} + 1 month + 25 days
Public Key reference	Public key of key pair DV_KEY_33
Signing Key reference	Signed with the private key of key pair CVCA_KEY_33

2.4.33.28 DV_CERT_33aa

ID	DV_CERT_33aa														
Purpose	This certificate is a regular domestic DV certificate which is issued by the CVCA.														
Version	Smart-eID														
Referred by	Test case EAC2 ISO7816_J_52														
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE033</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Official domestic DV, Read Access (all)</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_33</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_00</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE033	Certificate Holder Authorization	Official domestic DV, Read Access (all)	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_33	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETESTDVDE033														
Certificate Holder Authorization	Official domestic DV, Read Access (all)														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_33														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.33.29 DV_CERT_33bb

ID	DV_CERT_33bb														
Purpose	<p>Certificate with a wrong (short) public key.</p> <p>For RSA profile, same Algorithm Identifier but PK.DVCA's modulus length is shorter than the CVCA's key modulus length.</p> <p>For ECDSA profile, same Algorithm Identifier but DVCA's domain parameters are different and have a shorter prime length than the CVCA's key. The hash algorithm should be adapted if necessary.</p>														
Version	1.11														
Referred by	Test case EAC2_ISO7816_J_51														
Content definition	<pre> 7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 01 83 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj </pre> <p> <i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes) </p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>As defined by the CVCA</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTDVDE033</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Official domestic DV, Read Access (all)</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair DV_KEY_33bb</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair CVCA_KEY_00</td> </tr> </table>	Certification Authority Reference	As defined by the CVCA	Certificate Holder Reference	DETESTDVDE033	Certificate Holder Authorization	Official domestic DV, Read Access (all)	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair DV_KEY_33bb	Signing Key reference	Signed with the private key of key pair CVCA_KEY_00
Certification Authority Reference	As defined by the CVCA														
Certificate Holder Reference	DETESTDVDE033														
Certificate Holder Authorization	Official domestic DV, Read Access (all)														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair DV_KEY_33bb														
Signing Key reference	Signed with the private key of key pair CVCA_KEY_00														

2.4.33.30 AT_CERT_33

ID	AT_CERT_33
Purpose	This certificate defines a regular terminal certificate, which is issued by the DV_CERT_33. The cert grants access to all eID data groups.

Version	Smart-eID														
Referred by															
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 05 00 7F FF FF FF 5F 25 06 gg 5F 24 06 hh 5F 37 ii jj</p> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>														
Parameter	<table border="1"> <tr> <td>Certification Authority Reference</td> <td>DETESTDVDE033</td> </tr> <tr> <td>Certificate Holder Reference</td> <td>DETESTATDE033</td> </tr> <tr> <td>Certificate Holder Authorization</td> <td>Read access for all eID data groups</td> </tr> <tr> <td>Certificate effective date</td> <td>CVCA_{eff}</td> </tr> <tr> <td>Certificate expiration date</td> <td>CVCA_{eff} + 1 month</td> </tr> <tr> <td>Public Key reference</td> <td>Public key of key pair AT_KEY_33</td> </tr> <tr> <td>Signing Key reference</td> <td>Signed with the private key of key pair DV_KEY_33</td> </tr> </table>	Certification Authority Reference	DETESTDVDE033	Certificate Holder Reference	DETESTATDE033	Certificate Holder Authorization	Read access for all eID data groups	Certificate effective date	CVCA _{eff}	Certificate expiration date	CVCA _{eff} + 1 month	Public Key reference	Public key of key pair AT_KEY_33	Signing Key reference	Signed with the private key of key pair DV_KEY_33
Certification Authority Reference	DETESTDVDE033														
Certificate Holder Reference	DETESTATDE033														
Certificate Holder Authorization	Read access for all eID data groups														
Certificate effective date	CVCA _{eff}														
Certificate expiration date	CVCA _{eff} + 1 month														
Public Key reference	Public key of key pair AT_KEY_33														
Signing Key reference	Signed with the private key of key pair DV_KEY_33														

2.4.33.31 AT_CERT_33a

ID	AT_CERT_33a
Purpose	This certificate is a regular IS certificate, which is issued by the DV_CERT_33aa.
Version	Smart-eID
Referred by	Test case EAC2_ISO7816_J_51
Content definition	<p>7F 21 aa 7F 4E bb 5F 29 01 00 42 cc dd 7F 49 ee ff 5F 20 xx yy 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 05 00 7F FF</p>

	FF FF 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> 5F 37 <i>ii jj</i> <p><i>aa</i> is the encoded combined length of certificate body and signature objects <i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>
Parameter	Certification Authority Reference
	DETESTDVDE033
	Certificate Holder Reference
	DETESTSTATDE033
	Certificate Holder Authorization
	Read access for all eID data groups
	CVCA _{eff}
	Certificate effective date
	CVCA _{eff} + 14 days
	Public Key reference
	Public key of key pair AT_KEY_33
	Signing Key reference
	Signed with the private key of key pair DV_KEY_33

2.4.33.32 AT_CERT_33b

ID	AT CERT 33b
Purpose	<p>Certificate with a wrong (short) Public key.</p> <p>For RSA profile, same Algorithm Identifier but IS key modulus length is shorter than the DVCA's key modulus length.</p> <p>For ECDSA profile, same Algorithm Identifier but IS key domain parameters are different and have a shorter prime length than the DVCA's key. The hash algorithm should be adapted if necessary.</p>
Version	1.11
Referred by	Test case EAC2 ISO7816 J 52
Content definition	7F 21 <i>aa</i> 7F 4E <i>bb</i> 5F 29 01 00 42 <i>cc dd</i> 7F 49 <i>ee ff</i> 5F 20 <i>xx yy</i> 7F 4C 0E 06 09 04 00 7F 00 07 03 01 02 01 53 05 00 7F FF FF FF 5F 25 06 <i>gg</i> 5F 24 06 <i>hh</i> 5F 37 <i>ii jj</i> <p><i>aa</i> is the encoded combined length of certificate body and signature objects</p>

	<p><i>bb</i> is the encoded length of the certificate body object <i>cc</i> is the encoded length of the Certification Authority Reference <i>dd</i> is the placeholder for the Certification Authority Reference (cc bytes) <i>ee</i> is the encoded length of the certificate's public key, <i>ff</i> is the placeholder for the certificate's public key bytes (ee bytes), <i>xx</i> is the encoded length of the Certificate Holder Reference <i>yy</i> is the placeholder for the Certificate Holder Reference (xx bytes) <i>gg</i> is the placeholder for the BCD encoded effective date of the certificate <i>hh</i> is the placeholder for the BCD encoded expiration date of the certificate <i>ii</i> is the encoded length of the certificates signature object, <i>jj</i> is the placeholder for the certificates signature (ii bytes)</p>	
Parameter	Certification Authority Reference	DETESTDVDE033
	Certificate Holder Reference	DETESTIATDE033
	Certificate Holder Authorization	Read access for all eID data groups
	Certificate effective date	CVCA _{eff}
	Certificate expiration date	CVCA _{eff} + 14 days
	Public Key reference	Public key of key pair AT_KEY_33b
	Signing Key reference	Signed with the private key of key pair DV_KEY_33a

3 Tests for layer 6 (ISO 7816)

This chapter defines the additional tests required for the extended command set used by the extended access control mechanisms.

3.1 Test case notation

The test cases defined below specify a set of command APDU which have to be sent to the test sample. While same parts of these APDUs are fixed, other elements have variable values which cannot be defined in general. The variable parts are marked by placeholder values which have to be replaced by the actual values. The following placeholders commonly used and therefore defined here in a global manner. All other placeholders are defined within the corresponding test case definition.

Placeholder	Definition
<Lc>	The length byte containing the length of the APDU command data.
<Le>	The length byte containing the length of the requested response data. Depending on the size of <Lc> the <Le> element must consist of one or two bytes (extended length). See ISO/IEC 7816-4 5.2 “ <i>In any command APDU comprising both Lc and Le fields (see ISO/IEC 7816-3), short and extended length fields shall not be combined: either both of them are short, or both of them are extended.</i> ”
<Ne>	Like <Le>, but placeholder for encoding within secure messaging (Tag 97)
<L _{xy} >	The encoded length of the data object xy.
<Cryptogram>	The encrypted part of a Secure Messaging APDU. The data content of this cryptogram is defined in the corresponding test case definition.
<Checksum>	The cryptographic checksum which is calculated over the protected parts of the Secure Messaging command.
' '	This is a binary OR operation. A bitwise OR takes two bit patterns of equal length and performs the logical OR operation on each pair of corresponding bits. The result in each position is 0 if both bits are 0, while otherwise the result is 1.

3.2 General requirements

3.2.1 Security Status

According to the definition in the EAC 2.0 specification [R8] the Secure Messaging session MUST be aborted if and only if a secure messaging error occurs or a plain APDU is received.

In respect to the Chip Authentication mechanism the EAC 2.0 specification contains an additional specification about the security status:

3.4.2. Security Status

If Chip Authentication Version 2 was successfully performed, Secure Messaging is restarted using the derived session keys K_{MAC} and K_{Enc} . Otherwise, Secure Messaging is continued using the previously established session keys (PACE).

3.5.2. Security Status

If the key agreement step during Chip Authentication Version 3 was successfully performed, Secure Messaging is restarted using the derived session keys K_{MAC} and K_{Enc} .

Reference 1: Security Status definition in the EAC 2.0 specification

Based on these definitions, all responses received during the test cases MUST be coded in secure messaging context unless stated different in the test case. The test setup MUST check this and MUST verify the cryptographic checksum.

3.2.2 Extended length APDUs

If the size of cryptographic keys leads to certificates that exceed the size of a standard APDU, all appropriate commands have been performed as extended length APDUs. In this case, the Lc field consists of three bytes and the corresponding Le field consists of two or three bytes.

3.2.3 Command Chaining

Command chaining is only used for the General Authenticate command. For MRTD chips support of command chaining is REQUIRED and support for command chaining MUST be indicated in the historical bytes of the ATR/ATS or in the EF.ATR. For terminals support of command chaining is REQUIRED. A terminal SHOULD test whether or not the MRTD chip supports command chaining before using this option.

3.3 Unit test EAC2_ISO7816_H – Password Authenticated Connection Establishment (PACE)

This unit covers all tests about the PACE mechanism. This mechanism establishes Secure Messaging between an MRTD chip and a terminal based on weak (short) passwords with the following advantages:

- Strong session keys are provided independent of the strength of the password.
- The entropy of the password(s) used to authenticate the terminal can be very low (e.g. 6 digits are sufficient in general).

The complete PACE mechanism is tested including robustness tests with invalid input data.

A terminal is *unauthenticated* before successfully completing Terminal Authentication. Unauthenticated terminals may only perform PIN management operations according to the password (CAN, PIN, PUK), which is used during that process.

An Authentication Terminal with effective authorization for PIN management may perform PIN management operations after completing General Authentication Procedure.

Note: This test unit has to be performed for each PACE protocol suite specified in ICS.

3.3.1 Test case EAC2_ISO7816_H_1

Test – ID	EAC2 ISO7816_H_1
Purpose	Positive test with a valid Password Authenticated Connection Establishment process and an unauthenticated terminal using CAN password
Version	EAC2_1.02
Profile	PACE, NOT SMARTeID
Preconditions	1. None, card recently activated
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eID Card: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 02 84 <L₈₄> <PACE domain>' <ul style="list-style-type: none"> PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>' Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>' Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>'

	<p>6. To verify that the new session keys are valid, an arbitrary SM APDU is send to the chip.</p> <pre>'0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'</pre>
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7C}> '84' <L₈₄> <ephemeral public key> '90 00' 5. 7C <L_{7C}> '86' <L₈₆> <authentication token> '90 00' 6. '90 00' within a valid SM response

3.3.2 Test case EAC2_ISO7816_H_2

Test – ID	EAC2_ISO7816_H_2
Purpose	Positive test with a valid Password Authenticated Connection Establishment process and an unauthenticated terminal using PIN password
Version	EAC2_1.02
Profile	PACE
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card with PIN: <code>'00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>'</code> <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: <code>'10 86 00 00 <Lc> 7C 00 <Le>'</code> 3. Send the given General Authenticate APDU to the eID Card to map the nonce: <code>'10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>'</code> 4. Perform key agreement: <code>'10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>'</code> 5. Perform mutual authentication: <code>'00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>'</code> 6. To verify that the new session keys are valid, an arbitrary SM APDU is send to the chip. <code>'0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'</code>
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00'

Test plan for eID-Cards with EAC 2.0

	<ol style="list-style-type: none"> 3. 7C <L_{7c}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7c}> '84' <L₈₄> <ephemeral public key> '90 00' 5. 7C <L_{7c}> '86' <L₈₆> <authentication token> '90 00' 6. '90 00' within a valid SM response
--	--

3.3.3 Test case EAC2_ISO7816_H_3

Test – ID	EAC2 ISO7816 H 3
Purpose	Positive test with a valid Password Authenticated Connection Establishment process and an unauthenticated terminal using PUK password
Version	EAC2_1.02
Profile	PACE, NOT SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card with PUK password: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 04 84 <L₈₄> <PACE domain>'<ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7c}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7c}> 83 <L₈₃> <ephemeral public key> <Le>' 5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7c}> 85 <L₈₅> <authentication token> <Le>' 6. To verify that the new session keys are valid, an arbitrary SM APDU is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. '7C <L_{7c}> 80' <L₈₀> <encrypted nonce> '90 00' 3. '7C <L_{7c}> 82' <L₈₂> <mapping data> '90 00' 4. '7C <L_{7c}> 84' <L₈₄> <ephemeral public key> '90 00' 5. '7C <L_{7c}> 86' <L₈₆> <authentication token> '90 00' 6. '90 00' within a valid SM response

3.3.4 Test case EAC2_ISO7816_H_4_Template

Test – ID	EAC2 ISO7816 H 4 Template
Purpose	Positive test with a valid Password Authenticated Connection Establishment process and a defined terminal type, i. e. submitting CHAT for Terminal Authentication
Version	see Table 7
Profile	see Table 7
Preconditions	1. None, card recently activated
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eID Card: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 <TYPE> 84 <L₈₄> <PACE domain> 7F4C <L_{7F4C}> <CHAT>' <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. • CHAT contains an OID and DDO. Those values and password type are defined by Table 7. </p> <p>2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>'</p> <p>3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>'</p> <p>4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>'</p> <p>5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>'</p> <p>6. To verify that the new session keys are valid, an arbitrary SM APDU is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'</p>
Expected results	<p>1. '90 00'</p> <p>2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00'</p> <p>3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00'</p> <p>4. 7C <L_{7C}> '84' <L₈₄> <ephemeral public key> '90 00'</p> <p>5. 7C <L_{7C}> '86' <L₈₆> <authentication token> '87' <L₈₇> <Certification Authority Reference> '88' <L₈₈> <Certification Authority Reference> '90 00' (DO88 is conditional)</p> <p>6. '90 00' within a valid SM response</p>

Test case EAC2_ISO7816_H_4a to Test case EAC2_ISO7815_H_4g:

Test Case ID	Version	Profile	OID (terminal type)	DDO (relative authorization)	Pwd Type
EAC2_ISO7816_H_4a	EAC2_1.02	PACE, NOT SMARTeID	id-IS (Inspection System)	03	'01'
EAC2_ISO7816_H_4b	EAC2_1.02	PACE, NOT SMARTeID	id-IS (Inspection System)	03	'02'
EAC2_ISO7816_H_4c	EAC2_1.02	PACE, NOT SMARTeID	id-AT (Authentication Terminal)	3F 7F FF FF FF	'02'
EAC2_ISO7816_H_4d	EAC2_1.02	PACE	id-AT (Authentication Terminal)	3F 7F FF FF FF	'03'
EAC2_ISO7816_H_4e	EAC2_1.02	PACE, NOT SMARTeID	id-ST (Signature Terminal)	03	'02'
EAC2_ISO7816_H_4f	EAC2_1.02	PACE, NOT SMARTeID	id-ST (Signature Terminal)	03	'03'
EAC2_ISO7816_H_4g	EAC2_1.02	PACE, NOT SMARTeID	id-ST (Signature Terminal)	03	'04'

Table 7: Test cases EAC2_ISO7816_H_4

3.3.5 Test case EAC2_ISO7816_H_5_Template

Test – ID	EAC2_ISO7816_H_5_Template
Purpose	Negative test with a valid Password Authenticated Connection Establishment process, but Terminal Type indicated by Certificate Holder Authorization Template is not authorized to use referenced password
Version	see Table 8
Profile	see Table 8
Preconditions	1. None, card recently activated
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eID Card: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 <TYPE> 84 <L₈₄> <PACE domain> 7F4C <L_{7F4C}> <CHAT>' <ul style="list-style-type: none"> PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. CHAT contains an OID and DDO. Those values and password type are defined by Table 8.
Expected results	<ol style="list-style-type: none"> '6A 80' In case of Smart-eID, if the password is not supported by the DUT, error code '6A 88' is also allowed.

Test case EAC2_ISO7816_H_5a to Test case EAC2_ISO7815_H_5e:

Test Case ID	Version	Profile	OID (terminal type)	DDO (relative authorization)	Pwd Type
EAC2_ISO7816_H_5_a	EAC2_1.0	PACE, NOT SMARTeID	id-IS (Inspection System)	03	'03'
EAC2_ISO7816_H_5_b	EAC2_1.0	PACE, NOT SMARTeID	id-IS (Inspection System)	03	'04'
EAC2_ISO7816_H_5_c	EAC2_1.0	PACE	id-AT (Authentication Terminal)	3F 7F FF FF FF	'01'
EAC2_ISO7816_H_5_d	EAC2_1.0	PACE	id-AT (Authentication Terminal)	3F 7F FF FF FF	'04'
EAC2_ISO7816_H_5_e	EAC2_1.0	PACE, NOT SMARTeID	id-ST (Signature Terminal)	03	'01'

Table 8: Test cases EAC2_ISO7816_H_5

3.3.6 Test case EAC2_ISO7816_H_6_Template

Test – ID	EAC2_ISO7816_H_6_Template
Purpose	Negative test with a valid Password Authenticated Connection Establishment process and a defined terminal type, i. e. submitting CHAT for Terminal Authentication, but invalid password implying invalid authentication token
Version	see Table 9
Profile	see Table 9
Preconditions	1. None, card recently activated
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eID Card: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 <TYPE> 84 <L₈₄> <PACE domain> 7F4C <L_{7F4C}> <CHAT>' • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm.</p> <ul style="list-style-type: none"> • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. • CHAT contains an OID and DDO. Those values and password type are defined by Table 9. <p>2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>'</p> <p>3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>'</p> <p>4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>'</p> <p>5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>'</p>

Test plan for eID-Cards with EAC 2.0

	Use INVALID authentication token
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7C}> '84' <L₈₄> <ephemeral public key> '90 00' 5. '63 00', '63 CX' or checking error

Test case EAC2_ISO7816_H_6a to Test case EAC2_ISO7815_H_6g:

Test Case ID	Version	Profile	OID (terminal type)	DDO (relative authorization)	Pwd Type
EAC2_ISO7816_H_6a	EAC2_1.02	PACE, NOT SMARTeID	id-IS (Inspection System)	03	'01'
EAC2_ISO7816_H_6b	EAC2_1.02	PACE, NOT SMARTeID	id-IS (Inspection System)	03	'02'
EAC2_ISO7816_H_6c	EAC2_1.02	PACE, NOT SMARTeID	id-AT (Authentication Terminal)	3F 7F FF FF FF	'02'
EAC2_ISO7816_H_6d	EAC2_1.02	PACE	id-AT (Authentication Terminal)	3F 7F FF FF FF	'03'
EAC2_ISO7816_H_6e	EAC2_1.02	PACE, NOT SMARTeID	id-ST (Signature Terminal)	03	'02'
EAC2_ISO7816_H_6f	EAC2_1.02	PACE, NOT SMARTeID	id-ST (Signature Terminal)	03	'03'
EAC2_ISO7816_H_6g	EAC2_1.02	PACE, NOT SMARTeID	id-ST (Signature Terminal)	03	'04'

Table 9: Test cases EAC2_ISO7816_H_6

3.3.7 Test case EAC2_ISO7816_H_7

Test – ID	EAC2_ISO7816_H_7
Version	deleted in version 1.00 RC

3.3.8 Test case EAC2_ISO7816_H_8

Test – ID	EAC2_ISO7816_H_8
Version	deleted in version 1.00 RC

3.3.9 Test case EAC2_ISO7816_H_9

Test – ID	EAC2_ISO7816_H_9
Version	deleted in version 1.00 RC

3.3.10 Test case EAC2_ISO7816_H_10

Test – ID	EAC2_ISO7816_H_10
Version	deleted in version 1.00 RC

3.3.11 Test case EAC2_ISO7816_H_11

Test – ID	EAC2_ISO7816_H_11
Version	deleted in version 1.00 RC

3.3.12 Test case EAC2_ISO7816_H_12

Test – ID	EAC2_ISO7816_H_12
Version	deleted in version 1.00 RC

3.3.13 Test case EAC2_ISO7816_H_13

Test – ID	EAC2_ISO7816_H_13
Version	deleted in version 1.00 RC

3.3.14 Test case EAC2_ISO7816_H_14

Test – ID	EAC2_ISO7816_H_14
Version	deleted in version 1.00 RC

3.3.15 Test case EAC2_ISO7816_H_15

Test – ID	EAC2_ISO7816_H_15
Version	deleted in version 1.00 RC

3.3.16 Test case EAC2_ISO7816_H_16

Test – ID	EAC2_ISO7816_H_16
Version	deleted in version 1.00 RC

3.3.17 Test case EAC2_ISO7816_H_17

Test – ID	EAC2_ISO7816_H_17
-----------	-------------------

Version	deleted in version 1.00 RC
---------	----------------------------

3.3.18 Test case EAC2_ISO7816_H_18

Test – ID	EAC2_ISO7816_H_18
Version	deleted in version 1.00 RC

3.3.19 Test case EAC2_ISO7816_H_19

Test – ID	EAC2_ISO7816_H_19
Version	deleted in version 1.00 RC

3.3.20 Test case EAC2_ISO7816_H_20

Test – ID	EAC2_ISO7816_H_20
Version	deleted in version 1.00 RC

3.3.21 Test case EAC2_ISO7816_H_21

Test – ID	EAC2_ISO7816_H_21
Version	moved in version 1.00 RC to Test case EAC2_ISO7816_P_8a

3.3.22 Test case EAC2_ISO7816_H_22

Test – ID	EAC2_ISO7816_H_22
Version	deleted in version 1.00 RC, duplicate of Test case EAC2_ISO7816_P_4

3.3.23 Test case EAC2_ISO7816_H_23

Test – ID	EAC2_ISO7816_H_23
Purpose	Test with invalid PIN/Password reference
Version	EAC2_1.0
Profile	PACE
Preconditions	1. None, card recently activated
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eID Card with invalid pin reference: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 <invalid password reference> 84 <L₈₄> <PACE domain>'</p> <ul style="list-style-type: none"> • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. • The password reference (DO83) has been set to an invalid value. (see ICS, use '05' if not otherwise stated)
Expected results	1. '6A 88'

3.3.24 Test case EAC2_ISO7816_H_24

Test – ID	EAC2_ISO7816_H_24
Version	deleted in version 1.00 RC

3.3.25 Test case EAC2_ISO7816_H_25

Test – ID	EAC2_ISO7816_H_25
Version	deleted in version 1.00 RC

3.3.26 Test case EAC2_ISO7816_H_26

Test – ID	EAC2_ISO7816_H_26
Version	Deleted in version 0.99

3.3.27 Test case EAC2_ISO7816_H_27

Test – ID	EAC2_ISO7816_H_27
Version	deleted in version 1.00 RC

3.3.28 Test case EAC2_ISO7816_H_28

Test – ID	EAC2_ISO7816_H_28
Version	moved in version 1.00 RC to Test case EAC2_ISO7816_P_19

3.3.29 Test case EAC2_ISO7816_H_29

Test – ID	EAC2_ISO7816_H_29
Version	deleted in version 1.00 RC

3.3.30 Test case EAC2_ISO7816_H_30

Test – ID	EAC2_ISO7816_H_30
Version	deleted in version 1.00 RC

3.3.31 Test case EAC2_ISO7816_H_31

Test – ID	EAC2_ISO7816_H_31
Version	deleted in version 1.00 RC

3.3.32 Test case EAC2_ISO7816_H_32

Test – ID	EAC2_ISO7816_H_32
-----------	-------------------

Version	deleted in version 1.00 RC
---------	----------------------------

3.3.33 Test case EAC2_ISO7816_H_33

Test – ID	EAC2_ISO7816_H_33
Purpose	Test with an invalid ephemeral public key - different key size
Version	EAC2 1.02
Profile	PACE
Preconditions	<ol style="list-style-type: none"> None, card recently activated
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eID Card with PIN: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>' <ul style="list-style-type: none"> PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7c}> 81 <L₈₁> <mapping data> <Le>' Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7c}> 83 <L₈₃> <ephemeral public key> <Le>' <ul style="list-style-type: none"> The ephemeral public key MUST be generated with domain parameters specifying a different key size (e.g. for a 224 bit key in EF.CardAccess / EF.CardSecurity a 192 bit ephemeral key pair is created)
Expected results	<ol style="list-style-type: none"> '90 00' 7C <L_{7c}> '80' <L₈₀> <encrypted nonce> '90 00' 7C <L_{7c}> '82' <L₈₂> <mapping data> '90 00' Checking error or '63 00'. Since there are invalid domain parameters used to generate the ephemeral key pair, the key agreement process MUST always fail.

3.3.34 Test case EAC2_ISO7816_H_34

Test – ID	EAC2_ISO7816_H_34
Purpose	Test with an invalid ephemeral public key - providing a (0,0) public key
Version	EAC2 1.02
Profile	PACE, ECDH
Preconditions	<ol style="list-style-type: none"> None, card recently activated
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eID Card: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>'

	<ul style="list-style-type: none"> PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. <ol style="list-style-type: none"> Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7c}> 81 <L₈₁> <mapping data> <Le>' Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7c}> 83 <L₈₃> <ephemeral public key> <Le>'<ul style="list-style-type: none"> The ephemeral public key has both coordinates set to zero.
Expected results	<ol style="list-style-type: none"> '90 00' 7C <L_{7c}> '80' <L₈₀> <encrypted nonce> '90 00' 7C <L_{7c}> '82' <L₈₂> <mapping data> '90 00' Checking error or '63 00'. Even if public key validation is not done, ECDH computation SHOULD fail with this input.

3.3.35 Test case EAC2_ISO7816_H_35

Test – ID	EAC2 ISO7816 H 35
Purpose	Test with an invalid ephemeral public key - value strictly bigger than the prime
Version	EAC2 1.02
Profile	PACE, DH
Preconditions	<ol style="list-style-type: none"> None, card recently activated
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eID Card: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>'<ul style="list-style-type: none"> PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7c}> 81 <L₈₁> <mapping data> <Le>' Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7c}> 83 <L₈₃> <ephemeral public key> <Le>' Use an ephemeral public key with a wrong value (value strictly bigger than the

Test plan for eID-Cards with EAC 2.0

	prime), e. g. ephemeral public key = prime p + 1
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 4. Checking error or '63 00'.

3.3.36 Test case EAC2_ISO7816_H_36

Test – ID	EAC2 ISO7816 H 36
Purpose	Test with an invalid ephemeral public key – value does not belong to the curve
Version	EAC2 1.02
Profile	PACE, ECDH
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>'<ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>' The ephemeral public key does not belong to the curve.
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 4. Checking error or '63 00'.

3.3.37 Test case EAC2_ISO7816_H_37

Test – ID	EAC2 ISO7816 H 37
Purpose	Negative test with a valid Password Authenticated Connection Establishment process and an unauthenticated terminal using CAN password that must be rejected by Smart-eID
Version	Smart-eID
Profile	SMARTeID

Preconditions	1. None, card recently activated
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 02 84 <L₈₄> <PACE domain>' <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7c}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7c}> 83 <L₈₃> <ephemeral public key> <Le>' 5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7c}> 85 <L₈₅> <authentication token> <Le>' 6. To verify that the PACE session is not established, an arbitrary SM APDU is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' or checking error. If status word is a checking error, the following test steps can be ignored. 2. 7C <L_{7c}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7c}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7c}> '84' <L₈₄> <ephemeral public key> '90 00' 5. 7C <L_{7c}> '86' <L₈₆> <authentication token> '90 00' 6. Checking error

3.4 Unit EAC2_ISO7816_I - Chip Authentication

The chip authentication mechanism uses the manage security environment command to verify that the chip is genuine. The terminal and the eID Card generate a shared secret based on the public key data stored in EF.CardSecurity file of the document. This secret is used to derive new session keys for the continued secure messaging session. The genuineness of the MRTD chip is explicitly verified by the authentication token and implicitly verified by its ability to perform Secure Messaging using the new session keys. The test cases specified in this unit verify the correct implementation of the "MSE:Set AT" / "General Authentication" command pair.

Test plan for eID-Cards with EAC 2.0

EF.CardSecurity file may contain an optional key reference identifier. This is useful if the chip supports multiple keys for Chip Authentication. The MSE:Set AT command can be called either with implicit key selection if no key reference is included in EF.CardSecurity or with the explicit key reference defined in the EF.CardSecurity element. All tests in this unit SHOULD be used with implicit or explicit key reference depending on the presence of the key reference element in EF.CardSecurity.

The EF.CardSecurity may contain more than one ChipAuthenticationPublicKeyInfo. In this case, all appropriate tests must be performed for each key. The corresponding test case is only rated as a PASS if all passes are completed successfully. For test cases where the Chip Authentication mechanism is just used as precondition always the first key is used.

Depending on the context (eID or Smart-eID) Terminal Authentication in preconditions must be performed with certificate chain of IS-specific DV_CERT_1 and IS_CERT_1 or AT-specific DV_CERT_19 and AT_CERT_19. In case of Smart-eID protocol PACE MUST be performed with PIN.

3.4.1 Test case EAC2_ISO7816_I_1

Test - ID	EAC2_ISO7816_I_1
Purpose	MSE:Set AT / General Authenticate commands with correct ephemeral public key
Version	EAC2_1.0
Profile	(PACE, TA2_IS, CA2) or SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN. 2. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19). The ChipAuthenticationPublicKeyInfo stored in CardSecurity file MUST have been read to be able to generate an ephemeral key pair. 3. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card. '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <cryptographic mechanism reference> 84 <L₈₄> <private key reference> • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in EF.CardSecurity file. 2. Send the given General Authenticate APDU to the eID Card. '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> 3. Verify the returned authentication token TPICC 4. To verify the chips ability to continue the Secure Messaging with the new session keys, an arbitrary SM APDU is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys.

	<p>2. $7C <L_{7C}> '81 <L_{81}> <\text{Nonce}> 82 <L_{82}> <\text{Authentication Token}> 90\ 00'$ in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys.</p> <p>3. True</p> <p>4. '$90\ 00$' and a valid Secure Messaging response. The returned data MUST be encoded with the NEW session keys.</p>
--	--

3.4.2 Test case EAC2 ISO7816_I_2

Test - ID	EAC2 ISO7816_I_2
Purpose	MSE:Set AT / General Authenticate commands with correct ephemeral public key, but afterward the old session keys are used.
Version	EAC2_1.0
Profile	(PACE, TA2_IS, CA2) or SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN. 2. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19). 3. The ChipAuthenticationPublicKeyInfo stored in CardSecurity file MUST have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card. $'0C\ 22\ 41\ A4\ <Lc>\ 87\ <L_{87}>\ 01\ <\text{Cryptogram}>\ 8E\ 08\ <\text{Checksum}>\ 00'$ <ul style="list-style-type: none"> • $<\text{Cryptogram}>$ contains the following encrypted data objects $80\ <L_{80}>\ <\text{cryptographic mechanism reference}>$ $84\ <L_{84}>\ <\text{private key reference}>$ • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in EF.CardSecurity file. 2. Send the given General Authenticate APDU to the eID Card. $'0C\ 86\ 00\ 00\ <Lc>\ 87\ <L_{87}>\ 01\ <\text{Cryptogram}>\ 97\ <L_{97}>\ <\text{Ne}>\ 8E\ 08\ <\text{Checksum}>\ <Le>'$ <ul style="list-style-type: none"> • $<\text{Cryptogram}>$ contains the following encrypted data objects $7C\ <L_{7C}>\ 80\ <L_{80}>\ <\text{ephemeral public key}>$ 3. Verify the returned authentication token T_{PICC} 4. Instead of using the new session keys, the old session keys are used to send an arbitrary SM APDU to the chip. $'0C\ B0\ (80\ <\text{sfi.EF.CardAccess}>)\ 00\ 0D\ 97\ 01\ 01\ 8E\ 08\ <\text{checksum}>\ 00'$
Expected results	<ol style="list-style-type: none"> 1. '$90\ 00$' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 2. $7C <L_{7C}> '81 <L_{81}> <\text{Nonce}> 82 <L_{82}> <\text{Authentication Token}> 90\ 00'$ in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 3. True

	4. Checking error. The chip MUST delete the old session key and MUST NOT accept any APDUs with these session keys.
--	--

3.4.3 Test case EAC2_ISO7816_I_3

Test - ID	EAC2_ISO7816_I_3
Purpose	MSE:Set AT / General Authenticate commands with invalid ephemeral public key (different key size)
Version	EAC2_1.0
Profile	(PACE, TA2_IS, CA2) or SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN. 2. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19). 3. The ChipAuthenticationPublicKeyInfo stored in CardSecurity file MUST have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card. '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <cryptographic mechanism reference> 84 <L₈₄> <private key reference> • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the EF.CardSecurity file. 2. Send the given General Authenticate APDU to the eID Card. '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> • The ephemeral public key MUST be generated with domain parameters specifying a different key size (e.g. for a 224 bit key in EF.CardSecurity a 192 bit ephemeral key pair is created) 3. To verify that the old (PACE based) session keys can still be used, an arbitrary SM APDU is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 2. Checking error, or warning '63 00'. Since there are invalid domain parameters used to generate the ephemeral key pair, the key agreement process MUST always fail. 3. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys.

3.4.4 Test case EAC2_ISO7816_I_4

Test - ID	EAC2 ISO7816 I 4
Purpose	MSE:Set AT / General Authenticate commands with a valid ephemeral public key, but without SecureMessaging
Version	EAC2 1.0
Profile	(PACE, TA2_IS, CA2) or SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN. 2. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19). 3. The ChipAuthenticationPublicKeyInfo stored in EF.CardSecurity MUST have been read BEFORE to be able to generate an ephemeral key pair.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card. '00 22 41 A4 <Lc> 80 <L₈₀> <CA OID> 84 <L₈₄> <private key reference> <ul style="list-style-type: none"> • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the EF.CardSecurity file. 2. Send the given General Authenticate APDU to the eID Card. '00 86 00 00 <Lc> 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> <Le>' 3. To verify that the chip has deleted the old (PACE based) session keys, an arbitrary SM APDU is send to the chip '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' or Checking error. A chip may permit the use of an unprotected MSE APDU, however, the SM channel MUST be closed as soon as an unprotected APDU is send. Therefore, the response MUST be send without SM encoding. 2. Checking error. The error code SHALL be returned as plain data without SM encoding. 3. Checking error. The error code SHALL be returned as plain data without SM encoding.

3.4.5 Test case EAC2_ISO7816_I_5

Test - ID	EAC2 ISO7816 I 5
Purpose	MSE:Set AT / General Authenticate commands with correct ephemeral public key but invalid class byte
Version	EAC2 1.0
Profile	(PACE, TA2_IS, CA2) or SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN. 2. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19). 3. The ChipAuthenticationPublicKeyInfo stored in CardSecurity file MUST have

	<p>been read to be able to generate an ephemeral key pair.</p> <p>4. All commands are encoded as legally structured Secure Messaging APDUs.</p>
Test scenario	<ol style="list-style-type: none"> Send the given MSE:Set AT APDU to the eID Card. '8C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <cryptographic mechanism reference> 84 <L₈₄> <private key reference> The class byte has been set to an invalid value of 8C. The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the EF.CardSecurity file. Send the given General Authenticate APDU to the eID Card. '8C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> The class byte has been set to an invalid value of 8C.
Expected results	<ol style="list-style-type: none"> Checking error. Note that the behavior of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response. Checking error. Note that the behavior of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response.

3.4.6 Test case EAC2_ISO7816_I_6

Test - ID	EAC2_ISO7816_I_6
Purpose	MSE:Set AT / General Authenticate commands with invalid data object tag for the ephemeral public key
Version	EAC2 1.0
Profile	(PACE, TA2_IS, CA2) or SMARTeID
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed with PIN. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19). The ChipAuthenticationPublicKeyInfo stored in CardSecurity file MUST have been read to be able to generate an ephemeral key pair. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE:Set AT APDU to the eID Card. '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <cryptographic mechanism reference> 84 <L₈₄> <private key reference> The private key reference MUST be included in the APDU if and only if it is

	<p>specified in the ChipAuthenticationPublicKeyInfo structure stored in the EF.CardSecurity file.</p> <ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eID Card. '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 81 <L₈₁> <ephemeral public key> • The data object for the ephemeral public key has an invalid tag 81. 3. To verify that the old session keys are still valid, an arbitrary SM APDU is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 2. Checking error. The error MUST be encoded in a Secure Messaging response using the OLD session keys. 3. '90 00' and a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys.

3.4.7 Test case EAC2_ISO7816_I_7

Test - ID	EAC2_ISO7816_I_7
Purpose	MSE:Set AT command with wrongly appended le byte
Version	EAC2_1.0
Profile	(PACE, TA2_IS, CA2) or SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN. 2. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19). 3. The ChipAuthenticationPublicKeyInfo stored in CardSecurity file MUST have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card. '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 01 00 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <cryptographic mechanism reference> 84 <L₈₄> <private key reference> • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the EF.CardSecurity file. • The APDU has wrongly appended DO97 with an encoded Le byte. 2. To verify that the chip does not activate the new session keys, an arbitrary SM APDU using the OLD keys is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'

Expected results	<ol style="list-style-type: none"> 1. Checking error. Note that the Secure Messaging context is not affected by this error. Therefore this error must be encoded as an SM response. 2. '90 00' and a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys.
------------------	--

3.4.8 Test case EAC2_ISO7816_I_8

Test - ID	EAC2 ISO7816 I 8
Purpose	MSE:Set AT / General Authenticate commands with wrongly missing le byte in GA
Version	EAC2 1.03
Profile	(PACE, TA2_IS, CA2) or SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN. 2. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19). 3. The ChipAuthenticationPublicKeyInfo stored in CardSecurity file MUST have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card. '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <cryptographic mechanism reference> 84 <L₈₄> <private key reference> • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the EF.CardSecurity file. 2. Send the given General Authenticate APDU to the eID Card. '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> • The APDU has wrongly missing DO97. 3. To verify that the chip does not activate the new session keys, an arbitrary SM APDU using the OLD keys is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 2. Checking error. Note that the behavior of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response. 3. If Step 2 response is in plain a checking error is expected. Otherwise the expected result is '90 00' and a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys.

3.4.9 Test case EAC2_ISO7816_I_9

Test - ID	EAC2 ISO7816_I_9
Purpose	MSE:Set AT / General Authenticate commands, providing a (0,0) public key to General Authenticate
Version	EAC2_1.0
Profile	(PACE, TA2_IS, CA2, ECDH) or (SMARTeID, ECDH)
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN. 2. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19). 3. The ChipAuthenticationPublicKeyInfo stored in CardSecurity file MUST have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card. '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <cryptographic mechanism reference> 84 <L₈₄> <private key reference> • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the EF.CardSecurity file. 2. Send the given General Authenticate APDU to the eID Card. '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> • The public key has both coordinates set to zero. 3. To verify that the old session keys are still valid, an arbitrary SM APDU is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 2. Checking error or warning processing '63 00'. Note: Even if public key validation is not done, DH computation SHOULD fail with this input. The error MUST be encoded in a Secure Messaging response using the OLD session keys. 3. '90 00' and a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys.

3.4.10 Test case EAC2_ISO7816_I_10

Test - ID	EAC2 ISO7816_I_10
Purpose	MSE:Set AT / General Authenticate commands, test borderline cases for x- and y-coordinates (small x coordinate)

Test plan for eID-Cards with EAC 2.0

Version	EAC2_1.0
Profile	(PACE, TA2_IS, CA2, ECDH) or (SMARTeID, ECDH)
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN. 2. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19). 3. The ChipAuthenticationPublicKeyInfo stored in CardSecurity file MUST have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card. '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <cryptographic mechanism reference> 84 <L₈₄> <private key reference> • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the EF.CardSecurity file. 2. Send the given General Authenticate APDU to the eID Card. '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> • Use an ephemeral public key with an x-coordinate requiring less than $\lceil \log_{256} q \rceil$ bytes to be represented. Pad with zero bytes. (For details on q see [R6]) 3. Verify the returned authentication token T_{PICC} 4. To verify the chips ability to continue the Secure Messaging with the new session keys, an arbitrary SM APDU is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 2. '7C <L_{7C}> 81 <L₈₁> <Nonce> 82 <L₈₂> <Authentication Token> 90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 3. True 4. '90 00' and a valid Secure Messaging response. The returned data MUST be encoded with the new session keys.

3.4.11 Test case EAC2_ISO7816_I_11

Test - ID	EAC2_ISO7816_I_11
Purpose	MSE:Set AT / General Authenticate commands, test borderline cases for x- and y-coordinates (large x coordinate)
Version	EAC2_1.0
Profile	(PACE, TA2_IS, CA2, ECDH) or (SMARTeID, ECDH)

Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN. 2. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19). 3. The ChipAuthenticationPublicKeyInfo stored in CardSecurity file MUST have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card. '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <cryptographic mechanism reference> 84 <L₈₄> <private key reference> • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the EF.CardSecurity file. 2. Send the given General Authenticate APDU to the eID Card. '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> • Use an ephemeral public key with an x-coordinate having its highest bit set to 1 3. Verify the returned authentication token T_{PICC} 4. To verify the chips ability to continue the Secure Messaging with the new session keys, an arbitrary SM APDU is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 2. '7C <L_{7C}> 81 <L₈₁> <Nonce> 82 <L₈₂> <Authentication Token> 90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 3. True 4. '90 00' and a valid Secure Messaging response. The returned data MUST be encoded with the new session keys.

3.4.12 Test case EAC2_ISO7816_I_12

Test - ID	EAC2 ISO7816 I 12
Purpose	MSE:Set AT / General Authenticate commands, test borderline cases for x- and y-coordinates (small y coordinate)
Version	EAC2 1.0
Profile	(PACE, TA2_IS, CA2, ECDH) or (SMARTeID, ECDH)
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN. 2. The Terminal Authentication MUST have been performed with certificates

Test plan for eID-Cards with EAC 2.0

	<p>dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19).</p> <ol style="list-style-type: none"> 3. The ChipAuthenticationPublicKeyInfo stored in CardSecurity file MUST have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card. <code>'0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</code> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects <code>80 <L₈₀> <cryptographic mechanism reference></code> <code>84 <L₈₄> <private key reference></code> • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in the EF.CardSecurity file. 2. Send the given General Authenticate APDU to the eID Card. <code>'0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>'</code> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects <code>7C <L_{7C}> 80 <L₈₀> <ephemeral public key></code> • Use an ephemeral public key with a y-coordinate requiring less than $[\log_{256} q]$ bytes to be represented. Pad with zero bytes. (For details on q see [R6]) 3. Verify the returned authentication token T_{PICC} 4. To verify the chips ability to continue the Secure Messaging with the new session keys, an arbitrary SM APDU is send to the chip. <code>'0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'</code>
Expected results	<ol style="list-style-type: none"> 1. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 2. '7C <L_{7C}> 81 <L₈₁> <Nonce> 82 <L₈₂> <Authentication Token> 90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 3. True 4. '90 00' and a valid Secure Messaging response. The returned data MUST be encoded with the new session keys.

3.4.13 Test case EAC2_ISO7816_I_13

Test - ID	EAC2_ISO7816_I_13
Purpose	MSE:Set AT / General Authenticate commands, test borderline cases for x- and y-coordinates (large y coordinate)
Version	EAC2_1.0
Profile	(PACE, TA2_IS, CA2, ECDH) or (SMARTeID, ECDH)
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN. 2. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19).

	<ol style="list-style-type: none"> 3. The ChipAuthenticationPublicKeyInfo stored in CardSecurity file MUST have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card. '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <cryptographic mechanism reference> 84 <L₈₄> <private key reference> • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in EF.CardSecurity file. 2. Send the given General Authenticate APDU to the eID Card. '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> • Use an ephemeral public key with a y-coordinate having its highest bit set to 1 3. Verify the returned authentication token T_{PICC} 4. To verify the chips ability to continue the Secure Messaging with the new session keys, an arbitrary SM APDU is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 2. '7C <L_{7C}> 81 <L₈₁> <Nonce> 82 <L₈₂> <Authentication Token> 90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 3. True 4. '90 00' and a valid Secure Messaging response. The returned data MUST be encoded with the new session keys.

3.4.14 Test case EAC2_ISO7816_I_14

Test - ID	EAC2_ISO7816_I_14
Purpose	MSE:Set AT command with an incorrect private key reference Note: The support for key references is not mandatory for the chip. This test is set optional.
Version	EAC2_1.0
Profile	(PACE, TA2_IS, CA2) or SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN. 2. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19). 3. The ChipAuthenticationPublicKeyInfo stored in CardSecurity file MUST have

Test plan for eID-Cards with EAC 2.0

	<p>been read to be able to generate an ephemeral key pair.</p> <p>4. All commands are encoded as legally structured Secure Messaging APDUs.</p>
Test scenario	<ol style="list-style-type: none"> Send the given MSE:Set AT APDU to the eID Card. '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <cryptographic mechanism reference> 84 <L₈₄> <invalid private key reference> A private key reference MUST be included in the APDU. This key reference MUST be different from the one potentially specified in the ChipAuthenticationPublicKeyInfo structure stored in EF.CardSecurity file (see ICS). To verify that the old session keys are still valid, an arbitrary SM APDU is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	<ol style="list-style-type: none"> Checking error or warning processing '63 00'. The error MUST be encoded in a Secure Messaging response using the OLD session keys. '90 00' and a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys.

3.4.15 Test case EAC2_ISO7816_I_15

Test - ID	EAC2 ISO7816 I_15
Purpose	Check the Chip authentication failure (using DH) – wrong value (value strictly bigger than the Prime)
Version	EAC2 1.0
Profile	(PACE, TA2_IS, CA2, DH) or (SMARTeID, DH)
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed with PIN. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19). The ChipAuthenticationPublicKeyInfo stored in CardSecurity file MUST have been read to be able to generate an ephemeral key pair. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE:Set AT APDU to the eID Card. '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <cryptographic mechanism reference> 84 <L₈₄> <private key reference> The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in EF.CardSecurity file. Send the given General Authenticate APDU to the eID Card. '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇>'

	<p><Ne> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> • Use an ephemeral public key with a wrong value (value strictly bigger than the Prime) ephemeral public key = prime p + 1 <p>3. To verify that the old session keys are still valid, an arbitrary SM APDU is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 2. Checking error or warning processing '63 00'. The SW MUST be wrapped with the old session keys. Subsequent command MUST be wrapped with the old session keys. 3. '90 00' and a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys.

3.4.16 Test case EAC2_ISO7816_I_16

Test - ID	EAC2 ISO7816_I_16
Purpose	Check the Chip authentication failure (using ECDH) – wrong point (value does not belong to the curve)
Version	EAC2_1.0
Profile	(PACE, TA2_IS, CA2, ECDH) or (SMARTeID, ECDH)
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN. 2. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1 or TA2_AT: DV_CERT_19 and AT_CERT_19). 3. The ChipAuthenticationPublicKeyInfo stored in CardSecurity file MUST have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card. '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <cryptographic mechanism reference> 84 <L₈₄> <private key reference> • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in EF.CardSecurity file. 2. Send the given General Authenticate APDU to the eID Card. '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L₈₀> <ephemeral public key>

Test plan for eID-Cards with EAC 2.0

	<ul style="list-style-type: none"> • Use an ephemeral public key with a wrong point (value does not belong to the curve) <p>3. To verify that the old session keys are still valid, an arbitrary SM APDU is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 2. Checking error or warning processing '63 00'. The SW MUST be wrapped with the old session keys. Subsequent command MUST be wrapped with the old session keys. 3. '90 00' and a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys.

3.4.17 Test case EAC2_ISO7816_I_17

Test - ID	EAC2_ISO7816_I_17
Purpose	MSE:Set AT / General Authenticate commands with correct ephemeral public key using ChipAuthenticationPublicKeyInfo encapsulated in PrivilegedTerminalInfo
Version	EAC2_1.1
Profile	PACE, TA2_IS, CA2, CS
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN. 2. The Terminal Authentication MUST have been performed with certificates dependent on the context (TA2_IS: DV_CERT_1 and IS_CERT_1). 3. The ChipAuthenticationPublicKeyInfo encapsulated in PrivilegedTerminalInfo stored in ChipSecurity file MUST have been read to be able to generate an ephemeral key pair. 4. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card. '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <cryptographic mechanism reference> 84 <L₈₄> <private key reference> • The private key reference MUST be included in the APDU if and only if it is specified in the ChipAuthenticationPublicKeyInfo structure stored in EF.CardSecurity file. 2. Send the given General Authenticate APDU to the eID Card. '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> 3. Verify the returned authentication token TPICC 4. To verify that the old session keys are still valid, an arbitrary SM APDU is send to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08'

	<checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 2. 7C <L_{7C}> '81 <L₈₁> <Nonce> 82 <L₈₂> <Authentication Token> 90 00' in a valid Secure Messaging response. The returned data MUST be encoded with the OLD session keys. 3. The returned authentication token is valid. 4. '90 00' and a valid Secure Messaging response. The returned data MUST be encoded with the NEW session keys.

3.5 Unit EAC2_ISO7816_J - Certificate verification

During the Terminal Authentication process the certificate chain from the trust point returned by the PACE protocol down to the terminal certificate is verified. This is done by an alternating sequence of MSE: Set DST and Verify Certificate commands. This unit covers all certificate verification test cases which do NOT update the chips persistent memory. This means that all tests in this unit can be repeated with the same set of certificates.

PACE mechanism is performed with CAN (IS and ST) or PIN (AT including Smart-eID). Used Certificate Holder Authorization Template MUST match terminal type and authorization given by the certificate chain.

In case of Smart-eID the following CHAT should be used:

OID	id-AT OBJECT IDENTIFIER ::= {id-roles 2}
DO	3F FF FF FF F7 (all rights except Privileged Terminal are activated, two leading bits (39 and 38) are set to '0')

There is a note in preconditions of test cases where this CHAT should be used.

3.5.1 Test case EAC2_ISO7816_J_1_Template

Test - ID	EAC2_ISO7816_J_1_Template
Purpose	Positive test with a valid chain of CV certificates.
Version	see table 10
Profile	PACE or CAPA, see table 10
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs. 3. All response data MUST be SM protected.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 10.

	<pre>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> <p>3. Send the given MSE: Set DST APDU to the eID Card. <pre>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS/AT-Certificate as specified in table 10. <pre>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> </p> </p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_1a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_J_1b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33 and AT_CERT_33

Table 10: Test cases EAC2_ISO7816_J_1

3.5.2 Test case EAC2_ISO7816_J_2_Template

Test - ID	EAC2_ISO7816_J_2_Template
Purpose	Test with an invalid Certification Authority Reference.
Version	see table 11
Profile	PACE or CAPA, see table 11
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<p>1. Send the given MSE: Set DST APDU to the eID Card. <pre>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <BAD Certification Authority Reference> • The Certification Authority Reference returned by the PACE or CAPA mechanism is changed in the last character to create an invalid reference. </p>

	<p>2. Send the appropriate DV-Certificate as specified in table 11. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS/AT-Certificate as specified in table 11. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 2. Checking error or '6300' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '6300' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_2a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_J_2b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33 and AT_CERT_33

Table 11: Test cases EAC2_ISO7816_J_2

3.5.3 Test case EAC2_ISO7816_J_3_Template

Test - ID	EAC2_ISO7816_J_3_Template
Purpose	Test with an invalid certificate signature.
Version	see table 12
Profile	PACE or CAPA, see table 12
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card.

	<p>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. <ol style="list-style-type: none"> 2. Send the appropriate DV-Certificate as specified in see table 12. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <bad certificate signature> • The signature object of the certificate has been changed in last digit to make it invalid 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' 4. Send the appropriate IS/AT-Certificate as specified in see table 12. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or '63 00' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '63 00' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_3a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_J_3b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33 and AT_CERT_33

Table 12: Test cases EAC2_ISO7816_J_3

3.5.4 Test case EAC2_ISO7816_J_4_Template

Test - ID	EAC2_ISO7816_J_4_Template
-----------	---------------------------

Purpose	Test with a missing certificate signature.
Version	see table 13
Profile	PACE or CAPA, see table 13
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 13. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> • The certificate signature object is omitted. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-Certificate as specified in table 13. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or '63 00' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '63 00' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_4a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_J_4b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33 and AT_CERT_33

Table 13: Test cases EAC2_ISO7816_J_4

3.5.5 Test case EAC2_ISO7816_J_5_Template

Test - ID	EAC2_ISO7816_J_5_Template
Purpose	Test with a missing certificate body.
Version	see table 14
Profile	PACE or CAPA, see table 14
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 14. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 5F 37 <L_{5F37}> <certificate signature> • The certificate body object is omitted. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-Certificate as specified in table 14. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or '63 00' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '63 00' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_5a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1

EAC2_ISO7816_J_5b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33 and AT_CERT_33
-------------------	-----------	--------	---

Table 14: Test cases EAC2_ISO7816_J_5**3.5.6 Test case EAC2_ISO7816_J_6_Template**

Test - ID	EAC2 ISO7816 J 6 Template
Purpose	Test a DV certificate with a missing Holder Authorization.
Version	see table 15
Profile	PACE or CAPA, see table 15
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 15. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The certificate does not contain a certificate holder authorization 3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-Certificate as specified in table 15. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or '6300' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '6300' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust

	point for the IS/AT-Certificate verification.
--	---

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_6a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1a and IS_CERT_1
EAC2_ISO7816_J_6b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33a and AT_CERT_33

Table 15: Test cases EAC2_ISO7816_J_6

3.5.7 Test case EAC2_ISO7816_J_7_Template

Test - ID	EAC2_ISO7816_J_7_Template
Purpose	Test a DV certificate with a missing effective date.
Version	see table 16
Profile	PACE or CAPA, see table 16
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified table 16. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The certificate does not have a certificate effective date tag. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-Certificate as specified in table 16. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response

	<ol style="list-style-type: none"> 2. Checking error or ‘6300’ within a valid SM response. 3. ‘90 00’ or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or ‘6300’ within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.
--	---

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_7a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1b and IS_CERT_1
EAC2_ISO7816_J_7b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33b and AT_CERT_33

Table 16: Test cases EAC2_ISO7816_J_7

3.5.8 Test case EAC2_ISO7816_J_8_Template

Test - ID	EAC2_ISO7816_J_8_Template
Purpose	Test a DV certificate with a missing expiration date.
Version	see table 17
Profile	PACE or CAPA, see table 17
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. ‘0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00’ <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 17. ‘0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The certificate does not have a certificate expiration date tag. 3. Send the given MSE: Set DST APDU to the eID Card. ‘0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00’ <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-Certificate as specified in table 17. ‘0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08

	<p><Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or '6300' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '6300' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_8a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1c and IS_CERT_1
EAC2_ISO7816_J_8b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33c and AT_CERT_33

Table 17: Test cases EAC2_ISO7816_J_8

3.5.9 Test case EAC2_ISO7816_J_9_Template

Test - ID	EAC2_ISO7816_J_9_Template
Purpose	<p>Test a DV certificate with an incorrect encoded effective date (bad BCD coding). Note: The date format verification is not mandatory for the chip. This test is set optional.</p>
Version	see table 18
Profile	PACE or CAPA, DATE, see table 18
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 18. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The certificate contains a badly encoded BCD effective date. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08

	<p><Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS/AT-Certificate as specified in table 18. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or '63 00' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '63 00' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_9a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1d and IS_CERT_1
EAC2_ISO7816_J_9b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33d and AT_CERT_33

Table 18: Test cases EAC2_ISO7816_J_9

3.5.10 Test case EAC2_ISO7816_J_10_Template

Test - ID	EAC2_ISO7816_J_10_Template
Purpose	<p>Test a DV certificate with an incorrect encoded expiration date. (bad BCD coding)</p> <p>Note:</p> <p>The date format verification is not mandatory for the chip. This test is set optional.</p>
Version	see table 19
Profile	PACE or CAPA, DATE, see table 19
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 19. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08

	<p><Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The certificate contains a badly encoded BCD expiration date. <p>3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS/AT-Certificate as specified in table 19. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or '6300' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '6300' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_10a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1e and IS_CERT_1
EAC2_ISO7816_J_10b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33e and AT_CERT_33

Table 19: Test cases EAC2_ISO7816_J_10

3.5.11 Test case EAC2_ISO7816_J_11

Test - ID	EAC2_ISO7816_J_11
Purpose	Test the "Current Date" update mechanism with a new foreign IS certificate.
Version	EAC2_1.0
Profile	PACE, TA2_IS
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'

	<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 2” chapter as DV_CERT_2. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-certificate is marked as a foreign DV-certificate. <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS-Certificate as specified in the “Certificate Set 2” chapter as IS_CERT_2a. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This certificate has an advanced effective date. Since the DV certificate was marked as a foreign one, the chip MUST NOT update the current date. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. <p>5. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>6. Send the appropriate DV-Certificate as specified in the “Certificate Set 2” chapter as DV_CERT_2. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-certificate is marked as a foreign DV-certificate. <p>7. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08</p>
--	---

	<pre> <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 6 has to be used. 8. Send the appropriate IS-Certificate as specified in the “Certificate Set 2” chapter as IS_CERT_2b. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This certificate expiration date is BEFORE the effective date of the IS- Certificate used in step 4. </pre>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response. 2. '90 00' within a valid SM response. 3. '90 00' within a valid SM response. 4. '90 00' within a valid SM response. 5. '90 00' within a valid SM response. 6. '90 00' within a valid SM response. 7. '90 00' within a valid SM response. 8. '90 00' within a valid SM response. This certificate MUST still be accepted since the chip MUST NOT change the current date based on the foreign IS certificate.

3.5.12 Test case EAC2_ISO7816_J_12_Template

Test - ID	EAC2 ISO7816 J 12 Template
Purpose	Test with a valid chain of CV certificates but without using SecureMessaging.
Version	see table 20
Profile	PACE or CAPA, see table 20
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '00 22 81 B6 <Lc> 83 <Certification Authority Reference>' <ul style="list-style-type: none"> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. • The APDU is send in plain without Secure Messaging 2. Send the appropriate DV-Certificate as specified in table 20. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>

	<ul style="list-style-type: none"> The APDU is send as a valid SM APDU. After step 2, the passport is reset and the preconditions of this test case are reestablished. <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. The APDU is send as a valid SM APDU. <p>4. Send the appropriate IS/AT-Certificate as specified in table 20. `00 2A 00 BE <Lc> 7F 4E <L_{7F4E}> <body> 5F 37 <L_{5F37}> <signature>'</p> <p>5. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certificate Holder Reference stored inside the DV-Certificate sent in step 4 has to be used. The APDU is send as a valid SM APDU.
Expected results	<ol style="list-style-type: none"> '90 00' or Checking error. A chip may permit the use of an unprotected MSE APDU, however, the SM channel MUST be closed as soon as an unprotected APDU is send. Therefore, the response MUST be send without SM encoding. Checking error. Since the SM channel MUST have been closed in Step 1, the chip MUST return an error without SM encoding here. '90 00' within a valid SM response '90 00' or Checking error. A chip may permit the use of an unprotected PSO APDU, however, the SM channel MUST be closed as soon as an unprotected APDU is send. Therefore, the response MUST be send without SM encoding. Checking error. Since the SM channel MUST have been closed in Step 4, the chip MUST return an error without SM encoding here.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_12a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_J_12b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33 and AT_CERT_33

Table 20: Test cases EAC2_ISO7816_J_12

3.5.13 Test case EAC2_ISO7816_J_13

Test - ID	EAC2_ISO7816_J_13
Purpose	Test the MSE: Set DST command with an invalid class byte.
Version	EAC2_1.0

Profile	PACE or CAPA, TA2_IS or TA2_AT
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '8C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. • The class byte is set to an invalid value. 2. If the error code in step 1 was returned in a Secure Messaging response, verify that the secure messaging session has not been aborted. If a plain error code was returned, this step is skipped. Send an arbitrary SM APDU to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. Checking error. Note that the behavior of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response. 2. Skipped or '90 00' within a valid SM response.

3.5.14 Test case EAC2_ISO7816_J_14_Template

Test - ID	EAC2_ISO7816_J_14_Template
Purpose	Test the Verify Certificate command with an invalid class byte.
Version	see table 21
Profile	PACE or CAPA, see table 21
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All commands are encoded as legally structured Secure Messaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 21. '8C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • The class byte has been set to an invalid value ('8C'). 3. If the error code in step 2 was returned in a Secure Messaging response, verify

	<p>that the secure messaging session has not been aborted. If a plain error code was returned, this step is skipped.</p> <p>Send an arbitrary SM APDU to the chip.</p> <pre>'0C 0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'</pre>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response. 2. Checking error. Note that the behavior of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response. 3. Skipped or '90 00' in a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_14a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1
EAC2_ISO7816_J_14b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33

Table 21: Test cases EAC2_ISO7816_J_14

3.5.15 Test case EAC2_ISO7816_J_15_Template

Test - ID	EAC2_ISO7816_J_15_Template
Purpose	Test with an invalid certificate body tag.
Version	see table 22
Profile	PACE or CAPA, see table 22
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. <code>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</code> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects <code>83 <L₈₃> <Certification Authority Reference></code> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 22. <code>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</code> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects <code>7F 4F <L_{7F4F}> <certificate body> 5F 37 <L_{5F37}> <certificate signature></code> • The certificate body tag has been changed to '7F 4F' 3. Send the given MSE: Set DST APDU to the eID Card. <code>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</code> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects <code>83 <L₈₃> <Certification Authority Reference></code> • The Certificate Holder Reference stored inside the DV-Certificate sent in

	<p>step 2 has to be used.</p> <p>4. Send the appropriate IS/AT-Certificate as specified in table 22. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> </p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or '63 00' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '63 00' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_15a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_J_15b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33 and AT_CERT_33

Table 22: Test cases EAC2_ISO7816_J_15

3.5.16 Test case EAC2_ISO7816_J_16_Template

Test - ID	EAC2_ISO7816_J_16_Template
Purpose	Test with an invalid certificate signature tag.
Version	see table 23
Profile	PACE or CAPA, see table 23
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in see table 23. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 38 <L_{5F38}> <certificate signature> • The certificate signature tag has been changed to '5F 38'

	<p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4 . Send the appropriate IS/AT-Certificate as specified in see table 23. `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or '63 00' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '63 00' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_16a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_J_16b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33 and AT_CERT_33

Table 23: Test cases EAC2_ISO7816_J_16

3.5.17 Test case EAC2_ISO7816_J_17_Template

Test - ID	EAC2_ISO7816_J_17_Template
Purpose	Test a DV certificate with an incorrect Gregorian effective date. Note: The date format verification is not mandatory for the chip. This test is set optional.
Version	see table 24
Profile	PACE or CAPA, DATE, see table 24
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<p>1. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism.

	<ol style="list-style-type: none"> 2. Send the appropriate DV-Certificate as specified in table 24. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The certificate contains an invalid Gregorian effective date. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-Certificate as specified in table 24. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or '63 00' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '63 00' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_17a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1f and IS_CERT_1
EAC2_ISO7816_J_17b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33f and AT_CERT_33

Table 24: Test cases EAC2_ISO7816_J_17

3.5.18 Test case EAC2_ISO7816_J_18_Template

Test - ID	EAC2_ISO7816_J_18_Template
Purpose	Test a DV certificate with an incorrect Gregorian expiration date. Note: The date format verification is not mandatory for the chip. This test is set optional.
Version	see table 25
Profile	PACE or CAPA , DATE, see table 25
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.

Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in see table 25. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The certificate contains an invalid Gregorian expiration date. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-Certificate as specified in see table 25. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or '6300' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '6300' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_18a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1g and IS_CERT_1
EAC2_ISO7816_J_18b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33g and AT_CERT_33

Table 25: Test cases EAC2_ISO7816_J_18

3.5.19 Test case EAC2_ISO7816_J_19_Template

Test - ID	EAC2_ISO7816_J_19_Template
-----------	----------------------------

Test plan for eID-Cards with EAC 2.0

Purpose	Test a DV certificate with an expiration date BEFORE the effective date.
Version	see table 26
Profile	PACE or CAPA, see table 26
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 26. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The certificate contains an expiration date BEFORE the effective date. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-Certificate as specified in table 26. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or '6300' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '6300' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_19a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1h and IS_CERT_1
EAC2_ISO7816_J_19b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33h and AT_CERT_33

Table 26: Test cases EAC2_ISO7816_J_19**3.5.20 Test case EAC2_ISO7816_J_20_Template**

Test - ID	EAC2_ISO7816_J_20_Template
Purpose	Test correct removal of temporary keys.
Version	see table 27
Profile	PACE or CAPA, see table 27
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs. 3. All response data MUST be SM protected.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 27. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 3. Reset the chip and reestablish the PACE or CAPA mechanism Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-Certificate as specified in table 27. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response. 2. '90 00' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '6300' within a valid SM response. The temporary key of the DV certificate MUST have been deleted during the reset. Therefore it MUST NOT be possible to verify the IS/AT-Certificate based on this key.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_20a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_J_20b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33 and AT_CERT_33

Table 27: Test cases EAC2_ISO7816_J_20**3.5.21 Test case EAC2_ISO7816_J_21_Template**

Test - ID	EAC2_ISO7816_J_21_Template
Purpose	Test a DV certificate with invalid combination of OID and discretionary data object in the Certificate Holder Authorization element.
Version	see table 28
Profile	PACE or CAPA, see table 28
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 28. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The certificate has an invalid combination of OID (<id-AT>) and discretionary data object (structured like a relative authorization bit map for an IS) in the Certificate Holder Authorization element. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-Certificate as specified in table 28. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>

Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response. 2. Checking error or '6300' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '6300' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.
------------------	---

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_21a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1i and IS_CERT_1
EAC2_ISO7816_J_21b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33i and AT_CERT_33

Table 28: Test cases EAC2_ISO7816_J_21

3.5.22 Test case EAC2_ISO7816_J_22_Template

Test - ID	EAC2_ISO7816_J_22_Template
Purpose	Test a DV certificate invalid OID in the Public Key element.
Version	see table 29
Profile	PACE or CAPA, see table 29
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 29. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The certificate has an invalid OID in the Public Key element. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

Test plan for eID-Cards with EAC 2.0

	<p>4. Send the appropriate IS/AT-Certificate as specified in table 29.</p> <p>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response. 2. Checking error or '6300' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '6300' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_22a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1j and IS_CERT_1
EAC2_ISO7816_J_22b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33j and AT_CERT_33

Table 29: Test cases EAC2_ISO7816_J_22

3.5.23 Test case EAC2_ISO7816_J_23_Template

Test - ID	EAC2_ISO7816_J_23_Template
Purpose	Test the CVCA root key selection with a wrong name (CAR) - Current date not updated
Version	see table 30
Profile	PACE or CAPA, see table 30
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed with CHAT specified in the first paragraph of this chapter. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with a wrong CAR. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the encrypted wrong CVCA key Name. 2. Send the appropriate DV-Certificate as specified in table 30. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The certificate is issued by the CVCA whose selection SHOULD have failed. • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date.

	<ul style="list-style-type: none"> Reset the chip after this step and restore the preconditions for this test case before the next step is performed. <p>3. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with a correct CVCA key name (CAR).</p> <p>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted Name (CAR) The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. <p>4. Send the appropriate DV-Certificate as specified in table 30.</p> <p>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	<ol style="list-style-type: none"> '90 00' or Checking error within a valid SM response. A chip may permit the selection of an unknown key. Checking error or warning processing '63 00' within a valid SM response '90 00' within a valid SM response '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_23a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12a and DV_CERT_1
EAC2_ISO7816_J_23b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33k and AT_CERT_33

Table 30: Test cases EAC2_ISO7816_J_23**3.5.24 Test case EAC2_ISO7816_J_24_Template**

Test - ID	EAC2_ISO7816_J_24_Template
Purpose	Test a DV certificate with a wrong certificate body tag - Current date not updated
Version	see table 31
Profile	PACE or CAPA, see table 31
Preconditions	<ol style="list-style-type: none"> The PACE or CAPA mechanism MUST have been performed with CHAT specified in the first paragraph of this chapter. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the MSE: Set DST APDU to initiate the certificate verification '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted CVCA key Name (CAR) The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism.

	<p>2. Send the appropriate DV-Certificate as specified in table 31. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4F <L_{7F4F}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The tag of the certificate body is wrong. • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. <p>3. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with the CAR of the CVCA. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR) • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. <p>4. Send the appropriate DV-Certificate as specified in table 31. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or warning processing '63 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_24a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12b and DV_CERT_1
EAC2_ISO7816_J_24b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33l and AT_CERT_33

Table 31: Test cases EAC2_ISO7816_J_24

3.5.25 Test case EAC2_ISO7816_J_25_Template

Test - ID	EAC2_ISO7816_J_25_Template
Purpose	Test a DV certificate with a wrong certificate signature tag - Current date not updated
Version	see table 32
Profile	PACE or CAPA, see table 32
Preconditions	1. The PACE or CAPA mechanism MUST have been performed with CHAT

	<p>specified in the first paragraph of this chapter.</p> <p>2. All APDUs are sent as valid SecureMessaging APDUs.</p>
Test scenario	<p>1. Send the MSE: Set DST APDU to initiate the certificate verification '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the encrypted CVCA key Name (CAR). • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism.</p> <p>2. Send the appropriate DV-Certificate as specified in see table 32. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 38 <L_{5F38}> <certificate signature> • The tag of the certificate signature is wrong. • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed.</p> <p>3. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with the CAR of the CVCA. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the encrypted CVCA key Name (CAR) • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism.</p> <p>4. Send the appropriate DV-Certificate as specified in see table 32. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.</p>
Expected results	<p>1. '90 00' within a valid SM response 2. Checking error or warning processing '63 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response</p>

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_25a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12c and DV_CERT_1
EAC2_ISO7816_J_25b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33m and AT_CERT_33

Table 32: Test cases EAC2_ISO7816_J_25

3.5.26 Test case EAC2_ISO7816_J_26_Template

Test - ID	EAC2 ISO7816 J 26 Template
Purpose	Test a DV certificate with a wrong certificate body length - Current date not updated
Version	see table 33
Profile	PACE or CAPA, see table 33
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed with CHAT specified in the first paragraph of this chapter. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the MSE: Set DST APDU to initiate the certificate verification '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR). • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 33. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> - 1 <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The length of the certificate body is inconsistent. • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with the CAR of the CVCA. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR) • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 4. Send the appropriate DV-Certificate as specified in table 33. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or warning processing '63 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_26a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12d and DV_CERT_1
EAC2_ISO7816_J_26b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33n and AT_CERT_33

Table 33: Test cases EAC2_ISO7816_J_26**3.5.27 Test case EAC2_ISO7816_J_27_Template**

Test - ID	EAC2_ISO7816_J_27_Template
Purpose	Test a DV certificate with a wrong certificate signature length - Current date not updated
Version	see table 34
Profile	PACE or CAPA, see table 34
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed with CHAT specified in the first paragraph of this chapter. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the MSE: Set DST APDU to initiate the certificate verification. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR). • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 34. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> - 1 <certificate signature> • The length of the certificate signature is inconsistent. • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with the CAR of the CVCA. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR) • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 4. Send the appropriate DV-Certificate as specified in table 34. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>

	<ul style="list-style-type: none"> This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	<ol style="list-style-type: none"> '90 00' within a valid SM response Checking error or warning processing '63 00' within a valid SM response '90 00' within a valid SM response '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_27a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12e and DV_CERT_1
EAC2_ISO7816_J_27b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33o and AT_CERT_33

Table 34: Test cases EAC2_ISO7816_J_27

3.5.28 Test case EAC2_ISO7816_J_28_Template

Test - ID	EAC2 ISO7816 J 28 Template
Purpose	Test a DV certificate with a wrong certificate signature (Last byte increased by 1) - Current date not updated
Version	see table 35
Profile	PACE or CAPA, see table 35
Preconditions	<ol style="list-style-type: none"> The PACE or CAPA mechanism MUST have been performed. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the MSE: Set DST APDU to initiate the certificate verification '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the encrypted CVCA key Name (CAR). The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. Send the appropriate DV-Certificate as specified in table 35. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature + 1> The certificate signature is wrong. It is obtained by increasing a correct signature by one. This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. Reset the chip after this step and restore the preconditions for this test case before the next step is performed. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with the CAR of the CVCA. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'

	<ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR) • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. <p>4. Send the appropriate DV-Certificate as specified in table 35. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or warning processing '63 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_28a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12f and DV_CERT_1
EAC2_ISO7816_J_28b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33p and AT_CERT_33

Table 35: Test cases EAC2_ISO7816_J_28**3.5.29 Test case EAC2_ISO7816_J_29_Template**

Test - ID	EAC2 ISO7816 J 29 Template
Purpose	Test a DV certificate with a wrong certificate signature (Dropping last byte of the signature) - Current date not updated
Version	see table 36
Profile	PACE or CAPA, see table 36
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed with CHAT specified in the first paragraph of this chapter. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the MSE: Set DST APDU to initiate the certificate verification. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR). • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 36 `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>

	<ul style="list-style-type: none"> The certificate signature is wrong. It is obtained by dropping the last byte of the certificate signature (the length of the DO remains consistent) This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. Reset the chip after this step and restore the preconditions for this test case before the next step is performed. <p>3. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with the CAR of the CVCA. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the encrypted CVCA key Name (CAR) The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. <p>4. Send the appropriate DV-Certificate as specified in table 36. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2. </p> </p>
Expected results	<ol style="list-style-type: none"> '90 00' within a valid SM response Checking error or warning processing '63 00' within a valid SM response '90 00' within a valid SM response '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_29a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12g and DV_CERT_1
EAC2_ISO7816_J_29b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33q and AT_CERT_33

Table 36: Test cases EAC2_ISO7816_J_29

3.5.30 Test case EAC2_ISO7816_J_30_Template

Test - ID	EAC2 ISO7816 J 30 Template
Purpose	Test a DV certificate with a wrong certificate signature (Signature greater than the modulus) - Current date not updated
Version	see table 37
Profile	PACE or CAPA, RSA, see table 37
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the MSE: Set DST APDU to initiate the certificate verification. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'

	<ul style="list-style-type: none"> <Cryptogram> contains the encrypted CVCA key Name (CAR). The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. <p>2. Send the appropriate DV-Certificate as specified in table 37 `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> The certificate signature is wrong. It is obtained by setting the signature to a value greater than the modulus. The length of the signature MUST match the length of the modulus. This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. Reset the chip after this step and restore the preconditions for this test case before the next step is performed. <p>3. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with the CAR of the CVCA. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted CVCA key Name (CAR) The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. <p>4. Send the appropriate DV-Certificate as specified in table 37. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	<ol style="list-style-type: none"> '90 00' within a valid SM response Checking error or warning processing '63 00' within a valid SM response '90 00' within a valid SM response '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_30a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12o and DV_CERT_1
EAC2_ISO7816_J_30b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33x and AT_CERT_33

Table 37: Test cases EAC2_ISO7816_J_30**3.5.31 Test case EAC2_ISO7816_J_31_Template**

Test - ID	EAC2_ISO7816_J_31_Template
-----------	----------------------------

Test plan for eID-Cards with EAC 2.0

Purpose	Test a DV certificate with a wrong certificate signature ($r = 0$) - Current date not updated
Version	see table 38
Profile	PACE or CAPA, ECDSA, see table 38
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed with CHAT specified in the first paragraph of this chapter. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the MSE: Set DST APDU to initiate the certificate verification. <code>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</code> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR). • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in see table 38. <code>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</code> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects <code>7F 4E <L_{7F4E}> <certificate body></code> <code>5F 37 <L_{5F37}> <certificate signature></code> • The certificate signature is wrong. It is obtained by filling the 'r' part of the signature with '00'. The length of 'r' still matches the size of the prime. • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with the CAR of the CVCA. <code>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</code> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR) • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 4. Send the appropriate DV-Certificate as specified in see table 38. <code>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</code> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects <code>7F 4E <L_{7F4E}> <certificate body></code> <code>5F 37 <L_{5F37}> <certificate signature></code> • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or warning processing '63 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
--------------	---------	---------	--------------

EAC2_ISO7816_J_31a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12p and DV_CERT_1
EAC2_ISO7816_J_31b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33y and AT_CERT_33

Table 38: Test cases EAC2_ISO7816_J_31**3.5.32 Test case EAC2_ISO7816_J_32_Template**

Test - ID	EAC2_ISO7816_J_32_Template
Purpose	Test a DV certificate with a wrong certificate signature (s = 0) - Current date not updated
Version	see table 39
Profile	PACE or CAPA, ECDSA, see table 39
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed with CHAT specified in the first paragraph of this chapter. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the MSE: Set DST APDU to initiate the certificate verification. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR). • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 39. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The certificate signature is wrong. It is obtained by filling the 's' part of the signature with '00'. The length of 's' still matches the size of the prime. • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with the CAR of the CVCA. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR) • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 4. Send the appropriate DV-Certificate as specified in table 39. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>

	<ul style="list-style-type: none"> This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	<ol style="list-style-type: none"> '90 00' within a valid SM response Checking error or warning processing '63 00' within a valid SM response '90 00' within a valid SM response '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_32a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12q and DV_CERT_1
EAC2_ISO7816_J_32b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33z and AT_CERT_33

Table 39: Test cases EAC2_ISO7816_J_32

3.5.33 Test case EAC2_ISO7816_J_33_Template

Test - ID	EAC2_ISO7816_J_33_Template
Purpose	Test a DV certificate without selecting any root key - Current date not updated
Version	see table 40
Profile	PACE or CAPA, see table 40
Preconditions	<ol style="list-style-type: none"> The PACE or CAPA mechanism MUST have been performed with CHAT specified in the first paragraph of this chapter. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the appropriate DV-Certificate as specified in table 40. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> As no current key is selected, the certificate verification SHOULD fail. This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. Reset the chip after this step and restore the preconditions for this test case before the next step is performed. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with the CAR of the CVCA. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the encrypted CVCA key Name (CAR) The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. Send the appropriate DV-Certificate as specified in table 40. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects

	<p>7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature></p> <ul style="list-style-type: none"> This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	<ol style="list-style-type: none"> Checking error or warning processing '63 00' within a valid SM response '90 00' within a valid SM response '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_33a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12a and DV_CERT_1
EAC2_ISO7816_J_33b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33k and AT_CERT_33

Table 40: Test cases EAC2_ISO7816_J_33**3.5.34 Test case EAC2_ISO7816_J_34_Template**

Test - ID	EAC2_ISO7816_J_34_Template
Purpose	Test a DV certificate while the Public Key DO has a wrong OID field - Current date not updated
Version	see table 41
Profile	PACE or CAPA, see table 41
Preconditions	<ol style="list-style-type: none"> The PACE or CAPA mechanism MUST have been performed with CHAT specified in the first paragraph of this chapter. All APDUs are sent as valid SecureMessaging APDUs.

Test plan for eID-Cards with EAC 2.0

Test scenario	<ol style="list-style-type: none"> 1. Send the MSE: Set DST APDU to initiate the certificate verification. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR). • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 41 '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The Public Key DO in the certificate body contains an incorrect OID that does not indicate id-TA (0.4.0.127.0.7.2.2.3.x.y). • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with the CAR of the CVCA. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR) • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 4. Send the appropriate DV-Certificate as specified in table 41. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or warning processing '63 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_34a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12i and DV_CERT_1
EAC2_ISO7816_J_34b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33s and AT_CERT_33

Table 41: Test cases EAC2_ISO7816_J_34

3.5.35 Test case EAC2_ISO7816_J_35_Template

Test - ID	EAC2_ISO7816_J_35_Template
Purpose	Test a DV certificate while the Public Key DO has no OID field - Current date not updated
Version	see table 42
Profile	PACE or CAPA, see table 42
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed with CHAT specified in the first paragraph of this chapter. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the MSE: Set DST APDU to initiate the certificate verification. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR). • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in see table 42. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The Public Key DO in the certificate body does not contain an OID field. • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with the CAR of the CVCA. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR) • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 4. Send the appropriate DV-Certificate as specified in see table 42. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or warning processing '63 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_35a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12h and DV_CERT_1
EAC2_ISO7816_J_35b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33r and AT_CERT_33

Table 42: Test cases EAC2_ISO7816_J_35**3.5.36 Test case EAC2_ISO7816_J_36_Template**

Test - ID	EAC2_ISO7816_J_36_Template
Purpose	Test a DV certificate while the Public Key DO has no Public point field - Current date not updated
Version	see table 43
Profile	PACE or CAPA, ECDSA, see table 43
Preconditions	<ol style="list-style-type: none"> The PACE or CAPA mechanism MUST have been performed with CHAT specified in the first paragraph of this chapter. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the MSE: Set DST APDU to initiate the certificate verification. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the encrypted CVCA key Name (CAR). The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. Send the appropriate DV-Certificate as specified in see table 43. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> The Public Key DO in the certificate body does not contain any EC Public point field. This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. Reset the chip after this step and restore the preconditions for this test case before the next step is performed. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with the CAR of the CVCA. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the encrypted CVCA key Name (CAR) The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. Send the appropriate DV-Certificate as specified in see table 43. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'

	<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or warning processing '63 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_36a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12j and DV_CERT_1
EAC2_ISO7816_J_36b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33t and AT_CERT_33

Table 43: Test cases EAC2_ISO7816_J_36

3.5.37 Test case EAC2_ISO7816_J_37_Template

Test - ID	EAC2_ISO7816_J_37_Template
Purpose	Test a DV certificate while the Public Key DO has no Modulus field - Current date not updated
Version	see table 44
Profile	PACE or CAPA, RSA, see table 44
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the MSE: Set DST APDU to initiate the certificate verification. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR). • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in see table 44. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The Public Key DO in the certificate body does not contain any RSA Modulus field. • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. Send the MSE: Set DST APDU to initiate the certificate verification to the eID

	<p>Card with the CAR of the CVCA.</p> <p>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR) • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. <p>4. Send the appropriate DV-Certificate as specified in see table 44.</p> <p>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or warning processing '63 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_37a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12k and DV_CERT_1
EAC2_ISO7816_J_37b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33u and AT_CERT_33

Table 44: Test cases EAC2_ISO7816_J_37

3.5.38 Test case EAC2_ISO7816_J_38_Template

Test - ID	EAC2_ISO7816_J_38_Template
Purpose	Test a DV certificate while the Public Key DO has no public exponent field - Current date not updated
Version	see table 45
Profile	PACE or CAPA, RSA, see table 45
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the MSE: Set DST APDU to initiate the certificate verification. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR). • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in see table 45. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects

	<p>7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature></p> <ul style="list-style-type: none"> The Public Key DO in the certificate body does not contain any RSA public exponent field. This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. Reset the chip after this step and restore the preconditions for this test case before the next step is performed. <p>3. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with the CAR of the CVCA. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted CVCA key Name (CAR) The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. <p>4. Send the appropriate DV-Certificate as specified in see table 45. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	<ol style="list-style-type: none"> '90 00' within a valid SM response Checking error or warning processing '63 00' within a valid SM response '90 00' within a valid SM response '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_38a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12l and DV_CERT_1
EAC2_ISO7816_J_38b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33v and AT_CERT_33

Table 45: Test cases EAC2_ISO7816_J_38**3.5.39 Test case EAC2_ISO7816_J_39_Template**

Test - ID	EAC2_ISO7816_J_39_Template
Purpose	Test a DV certificate while the Public Key DO contains an unknown DO - Current date not updated
Version	see table 46
Profile	PACE or CAPA, see table 46
Preconditions	<ol style="list-style-type: none"> The PACE or CAPA mechanism MUST have been performed with CHAT specified in the first paragraph of this chapter. All APDUs are sent as valid SecureMessaging APDUs.

Test plan for eID-Cards with EAC 2.0

Test scenario	<ol style="list-style-type: none"> 1. Send the MSE: Set DST APDU to initiate the certificate verification. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR). • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 46. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The Public Key DO in the certificate body contains an unknown DO (tag '77'). • This certificate has an advanced effective date. Since the DV certificate failed, the chip MUST NOT update the current date. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 3. Send the MSE: Set DST APDU to initiate the certificate verification to the eID Card with the CAR of the CVCA. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted CVCA key Name (CAR) • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 4. Send the appropriate DV-Certificate as specified in table 46. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This certificate expiration date is BEFORE the effective date of the DV-Certificate used in step 2.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or warning processing '63 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_39a	EAC2_1.0	TA2_IS	Certificate Set 12: DV_CERT_12m and DV_CERT_1
EAC2_ISO7816_J_39b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33w and DV_CERT_33

Table 46: Test cases EAC2_ISO7816_J_39

3.5.40 Test case EAC2_ISO7816_J_40

Test - ID	EAC2_ISO7816_J_40
Purpose	Test the transition CVCA \Rightarrow IS key
Version	EAC2_1.0
Profile	PACE, TA2_IS
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs. 3. All response data MUST be SM protected.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate IS-Certificate as specified in the “Certificate Set 10” chapter as IS_CERT_10. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or status bytes '63 00' within a valid SM response

3.5.41 Test case EAC2_ISO7816_J_41

Test - ID	EAC2_ISO7816_J_41
Purpose	Test the transition CVCA \Rightarrow domestic DV \Rightarrow CVCA
Version	EAC2_1.0
Profile	PACE, TA2_IS
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs. 3. All response data MUST be SM protected.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10a.

Test plan for eID-Cards with EAC 2.0

	<p>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> <p>3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate CA-Certificate as specified in the "Certificate Set 10" chapter as LINK_CERT_10. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. Checking error or status bytes '63 00' within a valid SM response.

3.5.42 Test case EAC2_ISO7816_J_42

Test - ID	EAC2 ISO7816 J 42
Purpose	Test the transition CVCA \Rightarrow foreign DV \Rightarrow CVCA
Version	EAC2 1.0
Profile	PACE, TA2_IS
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs. 3. All response data MUST be SM protected.
Test scenario	<p>1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>2. Send the appropriate DV-Certificate as specified in the "Certificate Set 10" chapter as DV_CERT_10b. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body>

	<p>5F 37 <L_{5F37}> <certificate signature></p> <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate CA-Certificate as specified in the “Certificate Set 10” chapter as LINK_CERT_10. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. Checking error or status bytes '63 00' within a valid SM response.

3.5.43 Test case EAC2_ISO7816_J_43

Test - ID	EAC2 ISO7816 J 43
Purpose	Test the transition CVCA \Rightarrow domestic DV \Rightarrow domestic DV
Version	EAC2 1.0
Profile	PACE, TA2 IS
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs. 3. All response data MUST be SM protected.
Test scenario	<p>1. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10a. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08</p>

	<pre><Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10c. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature></pre>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. Checking error or status bytes '63 00' within a valid SM response.

3.5.44 Test case EAC2_ISO7816_J_44

Test - ID	EAC2_ISO7816_J_44
Purpose	Test the transition CVCA \Rightarrow domestic DV \Rightarrow foreign DV
Version	EAC2 1.0
Profile	PACE, TA2_IS
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs. 3. All response data MUST be SM protected.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10a. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference>

	<ul style="list-style-type: none"> The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4 . Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10d. ‘0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>’</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> ’90 00’ within a valid SM response ’90 00’ within a valid SM response ’90 00’ within a valid SM response Checking error or status bytes ’63 00’ within a valid SM response.

3.5.45 Test case EAC2_ISO7816_J_45

Test - ID	EAC2_ISO7816_J_45
Purpose	Test the transition CVCA \Rightarrow foreign DV \Rightarrow domestic DV
Version	EAC2_1.0
Profile	PACE, TA2_IS
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed. All APDUs are sent as valid SecureMessaging APDUs. All response data MUST be SM protected.
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card. ‘0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00’ <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certification Authority Reference MUST be used as returned by the PACE mechanism. Send the appropriate DV-Certificate as specified in the “Certificate Set 10” chapter as DV_CERT_10b. ‘0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> Send the given MSE: Set DST APDU to the eID Card. ‘0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00’ <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. Send the appropriate DV-Certificate as specified in the “Certificate Set 10”

	<p>chapter as DV_CERT_10c.</p> <p>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects <p>7F 4E <L_{7F4E}> <certificate body></p> <p>5F 37 <L_{5F37}> <certificate signature></p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response. 2. '90 00' within a valid SM response. 3. '90 00' within a valid SM response. 4. Checking error or status bytes '63 00' within a valid SM response.

3.5.46 Test case EAC2_ISO7816_J_46

Test - ID	EAC2 ISO7816 J 46
Purpose	Test the transition CVCA \Rightarrow foreign DV \Rightarrow foreign DV
Version	EAC2 1.0
Profile	PACE, TA2 IS
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs. 3. All response data MUST be SM protected.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects <p>83 <L₈₃> <Certification Authority Reference></p> <ul style="list-style-type: none"> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the "Certificate Set 10" chapter as DV_CERT_10b. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects <p>7F 4E <L_{7F4E}> <certificate body></p> <p>5F 37 <L_{5F37}> <certificate signature></p> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects <p>83 <L₈₃> <Certification Authority Reference></p> <ul style="list-style-type: none"> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate DV-Certificate as specified in the "Certificate Set 10" chapter as DV_CERT_10d. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'

	<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response. 2. '90 00' within a valid SM response. 3. '90 00' within a valid SM response. 4. Checking error or status bytes '63 00' within a valid SM response.

3.5.47 Test case EAC2_ISO7816_J_47

Test - ID	EAC2_ISO7816_J_47
Purpose	Test the transition CVCA \Rightarrow DV \Rightarrow IS \Rightarrow foreign DV
Version	EAC2 1.0
Profile	PACE, TA2_IS
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs. 3. All response data MUST be SM protected.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the "Certificate Set 11" chapter as DV_CERT_11a. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the "Certificate Set 11" chapter as IS_CERT_11a. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>

Test plan for eID-Cards with EAC 2.0

	<p>5. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. <p>6. Send the appropriate DV-Certificate as specified in the “Certificate Set 11” chapter as DV_CERT_11b. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response 5. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 6. Checking error or '63 00' within a valid SM response.

3.5.48 Test case EAC2_ISO7816_J_48

Test - ID	EAC2 ISO7816 J 48
Purpose	Test the transition CVCA \Rightarrow DV \Rightarrow IS \Rightarrow domestic DV
Version	EAC2 1.0
Profile	PACE, TA2_IS
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs. 3. All response data MUST be SM protected.
Test scenario	<p>1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 11” chapter as DV_CERT_11a. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body>

	<p>5F 37 <L_{5F37}> <certificate signature></p> <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS-Certificate as specified in the “Certificate Set 11” chapter as IS_CERT_11a. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> <p>5. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. <p>6. Send the appropriate DV-Certificate as specified in the “Certificate Set 11” chapter as DV_CERT_11c. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response 5. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 6. Checking error or '63 00' within a valid SM response.

3.5.49 Test case EAC2_ISO7816_J_49

Test - ID	EAC2 ISO7816 J 49
Purpose	Test the transition CVCA \Rightarrow DV \Rightarrow IS \Rightarrow IS
Version	EAC2_1.0
Profile	PACE, TA2_IS
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed.

Test plan for eID-Cards with EAC 2.0

	<ol style="list-style-type: none"> 2. All APDUs are sent as valid SecureMessaging APDUs. 3. All response data MUST be SM protected.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 11” chapter as DV_CERT_11a. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 11” chapter as IS_CERT_11a. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 5. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. 6. Send the appropriate IS-Certificate as specified in the “Certificate Set 11” chapter as IS_CERT_11b. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response

	<p>4. '90 00' within a valid SM response</p> <p>5. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose.</p> <p>6. Checking error or '63 00' within a valid SM response.</p>
--	--

3.5.50 Test case EAC2_ISO7816_J_50

Test - ID	EAC2 ISO7816 J 50
Purpose	Test the transition CVCA \Rightarrow DV \Rightarrow IS \Rightarrow CVCA
Version	EAC2_1.0
Profile	PACE, TA2_IS
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs. 3. All response data MUST be SM protected.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the "Certificate Set 11" chapter as DV_CERT_11a. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the "Certificate Set 11" chapter as IS_CERT_11a. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 5. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'

	<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. <p>6. Send the appropriate CVCA-Certificate as specified in the “Certificate Set 11” chapter as LINK_CERT_11a. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response 5. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 6. Checking error or '63 00' within a valid SM response.

3.5.51 Test case EAC2_ISO7816_J_51_Template

Test - ID	EAC2_ISO7816_J_51_Template
Purpose	Test a DV certificate with a wrong Public Key (shorter key length).
Version	see table 47
Profile	PACE or CAPA, see table 47
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism must have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference must be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 47. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The key length of this certificate is different to the CVCA public key. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'

	<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference given in the previous DVCA-Certificate sent. <p>4. Send the appropriate IS-Certificate as specified in table 47. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. Checking error or '63 00' within a valid SM response. 3. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 4. Checking error or '63 00' within a valid SM response. Since the DV certificate was not verified successfully, it MUST NOT be possible to use it as the trust point for the IS/AT-Certificate verification.

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_51a	EAC2_1.0	TA2_IS	Certificate Set 14: DV_CERT_14b and IS_CERT_14a
EAC2_ISO7816_J_51b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33bb and AT_CERT_33a

Table 47: Test cases EAC2_ISO7816_J_51

3.5.52 Test case EAC2_ISO7816_J_52_Template

Test - ID	EAC2_ISO7816_J_52_Template
Purpose	Test a IS/AT certificate with a wrong Public Key (shorter key length).
Version	see table 48
Profile	PACE or CAPA, see table 48
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism must have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<p>1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference must be used as returned by the PACE or CAPA mechanism. <p>2. Send the appropriate CA-Certificate as specified in see table 48. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects

	<p>7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature></p> <ol style="list-style-type: none"> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference given in the previous DVCA-Certificate sent. 4. Send the appropriate IS-Certificate as specified in see table 48. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • The key length of this certificate is different to the CVCA and DV certificates public keys.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. Checking error or '63 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_J_51a	EAC2_1.0	TA2_IS	Certificate Set 14: DV_CERT_14a and IS_CERT_14b
EAC2_ISO7816_J_51b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33aa and AT_CERT_33b

Table 48: Test cases EAC2_ISO7816_J_52

3.6 Unit EAC2_ISO7816_K Terminal Authentication

This unit tests the second part of the terminal authentication process. In this step, the terminal proves the possession of the private key which belongs to its certificate.

PACE mechanism is performed with CAN (IS and ST) or PIN (AT). Used Certificate Holder Authorization Template MUST match terminal type and authorization given by the certificate chain.

3.6.1 Test case EAC2_ISO7816_K_1

Test - ID	EAC2_ISO7816_K_1
Purpose	Positive test with a valid terminal authentication process
Version	see table 49
Profile	PACE or CAPA, see table 49
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.

Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 49 . '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-certificate as specified in table 49 dependent on the context (IS or AT). '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference> 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS/AT-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01/AT_KEY_01.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response

	5. '90 00' within a valid SM response 6. '<Eight bytes of random data> 90 00' within a valid SM response 7. '90 00' within a valid SM response
--	--

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_K_01a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_K_01b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_19 and AT_CERT_19a

Table 49: Test cases EAC2_ISO7816_K_01

3.6.2 Test case EAC2_ISO7816_K_2

Test - ID	EAC2_ISO7816_K_2
Purpose	Test with an invalid certificate reference for the MSE:Set AT command
Version	see table 50
Profile	PACE or CAPA, see table 50
Preconditions	1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L ₈₇ > 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 50. '0C 2A 00 BE <Lc> 87 <L ₈₇ > 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L _{7F4E} > <certificate body> 5F 37 <L _{5F37} > <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L ₈₇ > 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-certificate as specified in table 50. '0C 2A 00 BE <Lc> 87 <L ₈₇ > 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L _{7F4E} > <certificate body> 5F 37 <L _{5F37} > <certificate signature>

	<p>5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • To generate an invalid certification holder reference, the last character of the holder reference stored inside the IS-Certificate sent in step 4 is changed. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. If no error occurred yet, send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01/AT_KEY_01.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response 5. '90 00' or checking error within a valid SM response. Note that some chip OS accept the selection of an unavailable public key and return an error only when the public key is used for the selected purpose. 6. '<Eight bytes of random data> 90 00' within a valid SM response or Checking error 7. Checking error or '6300' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_K_02a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_K_02b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_19 and AT_CERT_19a

Table 50: Test cases EAC2_ISO7816_K_02

3.6.3 Test case EAC2_ISO7816_K_3

Test - ID	EAC2_ISO7816_K_3
Purpose	Test with a terminal authentication process without secure messaging
Version	see table 51
Profile	PACE or CAPA, see table 51
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. The APDU is step 1 - 6 are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08

Test plan for eID-Cards with EAC 2.0

	<pre><Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 51. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-Certificate as specified in table 51. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS/AT-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eID Card. '00 82 00 00 <Lc> <Terminal generated signature> • The APDU is sent in plain without SM encoding • The signature is created with the private key of IS_KEY_01/AT_KEY_01.</pre>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response 5. '90 00' within a valid SM response 6. '<Eight bytes of random data> 90 00' within a valid SM response 7. Checking error as a plain response (without Secure Messaging)

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_K_03a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_K_03b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_19 and AT_CERT_19a

Table 51: Test cases EAC2_ISO7816_K_03

3.6.4 Test case EAC2_ISO7816_K_4

Test - ID	EAC2_ISO7816_K_4
Purpose	Test that the effective access rights in a DV-Certificate are ignored, i.e. sending a terminal certificate is skipped during TA and an error is expected
Version	see table 52
Profile	PACE or CAPA, see table 52
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 52. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 3. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference > 91 <L₉₁> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 5. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of DV_KEY_01.

Test plan for eID-Cards with EAC 2.0

Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' or Checking error within a valid SM response 4. '<Eight bytes of random data> 90 00' or Checking error within a valid SM response 5. Checking error or '6300' within a valid SM response
------------------	---

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_K_04a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_K_04b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_19 and AT_CERT_19a

Table 52: Test cases EAC2_ISO7816_K_04

3.6.5 Test case EAC2_ISO7816_K_5

Test - ID	EAC2 ISO7816 K 5
Purpose	Test that the effective access rights in a CVCA-Certificate are ignored, i.e. sending any certificate is skipped during TA and an error is expected
Version	EAC2 1.0
Profile	PACE or CAPA, TA2_IS or TA2_AT
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference> 91 <L91> <Compressed Ephemeral Public Key> • The Certification Authority Reference as returned by the PACE or CAPA mechanism. 2. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 3. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of CVCA_KEY_00.
Expected results	<ol style="list-style-type: none"> 1. '90 00' or Checking error within a valid SM response 2. '<Eight bytes of random data> 90 00' or checking error within a valid SM response 3. Checking error or '6300' within a valid SM response

3.6.6 Test case EAC2_ISO7816_K_6

Test - ID	EAC2 ISO7816 K 6
Purpose	Test the external authenticate command with an invalid class byte
Version	see table 53
Profile	PACE or CAPA, see table 53
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All commands are encoded as legally structured Secure Messaging APDUs..
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 53. '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-Certificate as specified in table 53 . '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS/AT-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eID Card.

	<p>'8C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01/AT_KEY_01. • The class byte is set to an invalid value ('8C') <p>8. If the error code in step 7 was returned in a Secure Messaging response, verify that the secure messaging session has not been aborted. If a plain error code was returned, this step is skipped. Send an arbitrary SM APDU to the chip. '0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response 5. '90 00' within a valid SM response 6. '<Eight bytes of random data> 90 00' within a valid SM response 7. Checking error. Note that the behavior of the chip regarding the Secure Messaging context is undefined. Therefore this error can be returned in plain or as an SM response. 8. Skipped or '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_K_06a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_K_06b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_19 and AT_CERT_19a

Table 53: Test cases EAC2_ISO7816_K_06

3.6.7 Test case EAC2_ISO7816_K_7

Test - ID	EAC2 ISO7816 K 7
Purpose	Terminal authentication process with two Get Challenge commands (Using the first challenge)
Version	see table 54
Profile	PACE or CAPA, see table 54
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism.

	<p>2. Send the appropriate DV-Certificate as specified in table 54. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS/AT-Certificate as specified in table 54. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> <p>5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS/AT-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given a second Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>8. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01/AT_KEY_01. • The signature is based on the first challenge received in step 6.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response 5. '90 00' within a valid SM response 6. '<Eight bytes of random data> 90 00' within a valid SM response 7. '<Eight bytes of random data> 90 00' or Checking error within a valid SM response

	8. Checking error or '63 00' within a valid SM response
--	---

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_K_07a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_K_07b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_19 and AT_CERT_19a

Table 54: Test cases EAC2_ISO7816_K_07**3.6.8 Test case EAC2_ISO7816_K_8**

Test - ID	EAC2_ISO7816_K_8
Purpose	Terminal authentication process with short challenge
Version	see table 55
Profile	PACE or CAPA, see table 55
Preconditions	<ol style="list-style-type: none"> The PACE or CAPA mechanism MUST have been performed. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. Send the appropriate DV-Certificate as specified in table 55. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. Send the appropriate IS/AT-Certificate as specified in table 55. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'

	<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> The Certificate Holder Reference stored inside the IS/AT-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 07 8E 08 <Checksum> 00'</p> <p>7. If the chip returns a short challenge (only 7 bytes) then send the given external authenticate command to the eID Card, otherwise skip this step. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01/AT_KEY_01. The signature is based on the short challenge received in step 6.
Expected results	<ol style="list-style-type: none"> '90 00' within a valid SM response '<Seven bytes of random data> 90 00' within a valid SM response or Checking error Skipped, Checking error or warning processing '63 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_K_08a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_K_08b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_19 and AT_CERT_19a

Table 55: Test cases EAC2_ISO7816_K_08

3.6.9 Test case EAC2_ISO7816_K_9

Test - ID	EAC2_ISO7816_K_9
Purpose	Check the Terminal authentication – No Get Challenge Performed
Version	see table 56
Profile	PACE or CAPA , TA2_IS or TA2_AT
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<p>1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference>

	<ul style="list-style-type: none"> The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. <p>2. Send the appropriate DV-Certificate as specified in table 56. '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> <p>3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS/AT-Certificate as specified in table 56. '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> <p>5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> The Certificate Holder Reference stored inside the IS/AT-Certificate sent in step 4 has to be used. <p>6. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01/AT_KEY_01. The wrong signature is calculated without any challenge. <p>7. Perform CA2</p>
Expected results	<ol style="list-style-type: none"> '90 00' within a valid SM response Checking error or warning processing '63 00' within a valid SM response. Checking error within a valid SM response during CA2

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_K_09a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_K_09b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_19 and AT_CERT_19a

Table 56: Test cases EAC2_ISO7816_K_09**3.6.10 Test case EAC2_ISO7816_K_10**

Test - ID	EAC2 ISO7816 K_10
Purpose	Check the Terminal authentication – No authentication key selection performed
Version	see table 57
Profile	PACE or CAPA, see table 57
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 57. '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-Certificate as specified in table 57. '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 5. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 6. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'

	<ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01/AT_KEY_01. • The signature is based on the challenge received in step 5. <p>7. Perform CA2</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response 5. '<Eight bytes of random data> 90 00' or checking error within an SM response 6. Checking error or warning processing '63 00' within a valid SM response 7. Checking error within a valid SM response during CA2

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_K_10a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_K_10b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_19 and AT_CERT_19a

Table 57: Test cases EAC2_ISO7816_K_10

3.6.11 Test case EAC2_ISO7816_K_11

Test - ID	EAC2_ISO7816_K_11
Purpose	Check the Terminal authentication – Wrong structure in the MSE: Set AT command
Version	see table 58
Profile	PACE or CAPA, see table 58
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 58. '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference>

	<ul style="list-style-type: none"> The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4 . Send the appropriate IS/AT-Certificate as specified in table 58. `0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> <p>5 . Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 84 <L84> <Certificate Holder Reference > instead of tag 83 91 <L91> <Compressed Ephemeral Public Key> The Certificate Holder Reference stored inside the IS/AT-Certificate sent in step 4 has to be used. <p>6 . Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7 . Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01/AT_KEY_01. The signature is based on the challenge received in step 6. <p>8 . Perform CA2</p> </p></p></p>
Expected results	<ol style="list-style-type: none"> '90 00' within a valid SM response Checking error within a valid SM response '<Eight bytes of random data> 90 00' or checking error within an SM response Checking error or warning processing '63 00' within a valid SM response Checking error within a valid SM response during CA2

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_K_11a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_K_11b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_19 and AT_CERT_19a

Table 58: Test cases EAC2_ISO7816_K_11

3.6.12 Test case EAC2_ISO7816_K_12

Test - ID	EAC2 ISO7816 K 12
Purpose	Check the Terminal authentication – Reset of the access rights in case of Application reset
Version	see table 59
Profile	PACE or CAPA, see table 59
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 59. '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-Certificate as specified in table 59. '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS/AT-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'

	<p>7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01/AT_KEY_01. • The signature is based on the challenge received in step 6. <p>8. Reset the chip by switching off the field and switching it on again</p> <ul style="list-style-type: none"> • Perform the PACE or CAPA mechanism • Perform CA2
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response 5. '90 00' within a valid SM response 6. '<Eight bytes of random data> 90 00' within an SM response 7. '90 00' within a valid SM response 8. Checking error within a valid SM response during CA2

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_K_12a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_K_12b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_19 and AT_CERT_19a

Table 59: Test cases EAC2_ISO7816_K_12

3.6.13 Test case EAC2_ISO7816_K_13

Test - ID	EAC2_ISO7816_K_13
Purpose	This test case checks if the chip does not accept more than one execution of Terminal Authentication within the same session, same certificate set.
Version	see table 60
Profile	PACE or CAPA, see table 60
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. The Terminal Authentication mechanism MUST have been performed based on the certificates specified in table 60. 3. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 60.

Test plan for eID-Cards with EAC 2.0

	<pre>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> <p>3. Send the given MSE: Set DST APDU to the eID Card. <pre>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS/AT-Certificate as specified in table 60. <pre>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> <p>5. Send the given MSE: Set AT APDU to the eID Card. <pre>'0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference> 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS/AT-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. <pre>'0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</pre> <p>7. Send the given external authenticate command to the eID Card. <pre>'0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature </p> </p></p></p></p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response 5. '90 00' or Checking error within a valid SM response. If this step returns Checking error the following steps don't need to be performed. 6. '<Eight bytes of random data> 90 00' within an SM response 7. Checking error within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_K_13a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1

EAC2_ISO7816_K_13b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_19 and AT_CERT_19a
--------------------	-----------	--------	--

Table 60: Test cases EAC2_ISO7816_K_13**3.6.14 Test case EAC2_ISO7816_K_14**

Test - ID	EAC2 ISO7816 K_14
Purpose	This test case checks if the chip does not accept more than one execution of Terminal Authentication within the same session, different certificate sets.
Version	see table 61
Profile	PACE or CAPA, see table 61
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. The Terminal Authentication mechanism MUST have been performed (in case of IS: DV_CERT_3, IS_CERT_3a; in case of AT: DV_CERT_20 and AT_CERT_20a). 3. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 2. Send the appropriate DV-Certificate as specified in table 61. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS/AT-Certificate as specified in table 61. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects

	<p>80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key></p> <ul style="list-style-type: none"> The Certificate Holder Reference stored inside the IS/AT-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature
Expected results	<ol style="list-style-type: none"> '90 00' within a valid SM response '90 00' or Checking error within a valid SM response. If this step returns Checking error the following steps don't need to be performed. '<Eight bytes of random data> 90 00' within an SM response Checking error within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_K_14a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_K_14b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_19 and AT_CERT_19a

Table 61: Test cases EAC2_ISO7816_K_14

3.6.15 Test case EAC2_ISO7816_K_15

Test - ID	EAC2 ISO7816 K 15
Purpose	This test case checks if the chip does not accept more than one execution of Terminal Authentication within the same session, different auxiliary data.
Version	EAC2_1.0
Profile	PACE or CAPA, TA2_AT
Preconditions	<ol style="list-style-type: none"> The PACE or CAPA mechanism MUST have been performed. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17f). Auxiliary data with valid Date of Birth data object MUST have been sent by authorized terminal during Terminal Authentication mechanism. Date of birth MUST NOT fit the required age. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects

	<p>83 <L83> <Certification Authority Reference></p> <ul style="list-style-type: none"> The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. <p>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 17” chapter as DV_CERT_17. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate AT-Certificate as specified in the “Certificate Set 17” chapter as AT_CERT_17f. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> <p>5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference> 91 <L91> <Compressed Ephemeral Public Key> 67 <L67> <Auxiliary Data> The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. Auxiliary data with valid Date of Birth data object MUST fit the required age. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature
Expected results	<ol style="list-style-type: none"> '90 00' within a valid SM response '90 00' or Checking error within a valid SM response. If this step returns

	<p>Checking error the following steps don't need to be performed.</p> <ol style="list-style-type: none"> 6. '<Eight bytes of random data> 90 00' within an SM response 7. Checking error within a valid SM response
--	---

3.6.16 Test case EAC2_ISO7816_K_16

Test - ID	EAC2 ISO7816 K_16
Purpose	Positive test with a valid terminal authentication process, but different order of commands (Get Challenge performed as first step in protocol)
Version	see table 62
Profile	PACE or CAPA, see table 62
Preconditions	<ol style="list-style-type: none"> 1. The PACE or CAPA mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 2. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE or CAPA mechanism. 3. Send the appropriate DV-Certificate as specified in table 62. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 4. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 5. Send the appropriate IS/AT-Certificate as specified in table 62. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 6. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08'

	<p><Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference> 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS/AT-Certificate sent in step 4 has to be used. <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' where the challenge of step 1 is used.</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01/AT_KEY_01.
Expected results	<ol style="list-style-type: none"> 1. '<Eight bytes of random data> 90 00' within a valid SM response 2. '90 00' within a valid SM response 3. '90 00' within a valid SM response 4. '90 00' within a valid SM response 5. '90 00' within a valid SM response 6. '90 00' within a valid SM response 7. '90 00' within a valid SM response

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_K_16a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_K_16b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_19 and AT_CERT_19a

Table 62: Test cases EAC2_ISO7816_K_16

3.7 Unit EAC2_ISO7816_L Effective Access Conditions

This unit tests evaluation of the effective access conditions, which has to be done by the chip. The chip has to grant access to sensitive data only if the complete terminal authentication mechanism has been performed. Furthermore, the access to the specific data groups depends on the access condition flags encoded in the DV and terminal certificate.

All tests described here use following OIDs and DDOs within the PACE mechanism (tag '7F 4C'):

Profile	OID (terminal type)	DDO (relative authorization)
ePassport	id-IS (Inspection System)	23
eID	id-AT (Authentication Terminal)	3E 1F FF FF F7
eSign	id-ST (Signature Terminal)	03

These CHATs do not restrict access to any functionality.

Because eSign functionality is specified separately, the special functions "Install Qualified Certificate" and "Install Advanced Certificate" are not tested here.

3.7.1 Test case EAC2_ISO7816_L_1

Test - ID	EAC2 ISO7816 L 1
Purpose	Positive test with a valid terminal authentication process with access permission for DG 3 if the DV certificate permits access to DG 3 and DG 4 while the IS certificate enables only the access to DG 3.
Version	EAC2 1.0
Profile	ePassport, TA2_IS, DG3
Preconditions	<ol style="list-style-type: none"> 1. The PACE (MRZ) mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 3” chapter as DV_CERT_3. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This DV-Certificate grants access to data group 3 and 4. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 3” chapter as IS_CERT_3a. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This IS-Certificate grants only access to data group 3. 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key>

	<ul style="list-style-type: none"> The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_03. </p> <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting ePassport application): `0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the encrypted ePassport application-ID. </p> <p>10. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 3 has been granted. `0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'</p>
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. '90 00' within a valid Secure Messaging response. true '90 00' within a valid Secure Messaging response. '<first byte of data group 3 content data> 90 00' within a valid Secure Messaging response.

3.7.2 Test case EAC2_ISO7816_L_2

Test - ID	EAC2_ISO7816_L_2
Purpose	Test that data group 4 cannot be accessed if the DV certificate permits access to DG 3 and DG 4 while the IS certificate enables only the access to DG 3.
Version	EAC2 1.0
Profile	ePassport, TA2_IS, DG4
Preconditions	<ol style="list-style-type: none"> The PACE (MRZ) mechanism MUST have been performed. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certification Authority Reference MUST be used as returned by the

	<p>PACE mechanism.</p> <ol style="list-style-type: none"> 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 3” chapter as DV_CERT_3. ‘0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This DV-Certificate grants access to data group 3 and 4. 3. Send the given MSE: Set DST APDU to the eID Card. ‘0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00’ <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 3” chapter as IS_CERT_3a. ‘0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This IS-Certificate grants only access to data group 3. 5. Send the given MSE: Set AT APDU to the eID Card. ‘0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00’ <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eID Card. ‘0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’ 7. Send the given external authenticate command to the eID Card. ‘0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_03. 8. The Chip Authentication mechanism MUST be performed. 9. Send the given Select Application APDU to the eID Card (selecting ePassport application): ‘0C A4 04 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ePassport application-ID. 10. Send the given Read Binary (with SFI) command to the eID Card, to verify the
--	--

	access to the data group 4 has NOT been granted. '0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. true 9. '90 00' within a valid Secure Messaging response. 10. Checking error within a valid Secure Messaging response.

3.7.3 Test case EAC2_ISO7816_L_3

Test - ID	EAC2 ISO7816 L 3
Purpose	Positive test with a valid terminal authentication process with access permission for DG 4 if the DV certificate permits access to DG 3 and DG 4 while the IS certificate enables only the access to DG 4.
Version	EAC2 1.0
Profile	ePassport, TA2_IS, DG4
Preconditions	<ol style="list-style-type: none"> 1. The PACE (MRZ) mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 3” chapter as DV_CERT_3 '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This DV-Certificate grants access to data group 3 and 4. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used.

	<ol style="list-style-type: none"> 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 3” chapter as IS_CERT_3b. ‘0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This IS-Certificate grants only access to data group 4. 5. Send the given MSE: Set AT APDU to the eID Card. ‘0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00’ <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eID Card. ‘0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’ 7. Send the given external authenticate command to the eID Card. ‘0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>’ <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_03. 8. The Chip Authentication mechanism MUST be performed. 9. Send the given Select Application APDU to the eID Card (selecting ePassport application): ‘0C A4 04 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’ <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ePassport application-ID. 10. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 4 has been granted. ‘0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00’
Expected results	<ol style="list-style-type: none"> 1. ‘90 00’ within a valid Secure Messaging response. 2. ‘90 00’ within a valid Secure Messaging response. 3. ‘90 00’ within a valid Secure Messaging response. 4. ‘90 00’ within a valid Secure Messaging response. 5. ‘90 00’ within a valid Secure Messaging response. 6. ‘<Eight bytes of random data> 90 00’ within a valid Secure Messaging response. 7. ‘90 00’ within a valid Secure Messaging response. 8. true 9. ‘90 00’ within a valid Secure Messaging response. 10. ‘<first byte of data group 4 content data> 90 00’ within a valid Secure Messaging response.

3.7.4 Test case EAC2_ISO7816_L_4

Test - ID	EAC2 ISO7816 L 4
Purpose	Test that data group 3 cannot be accessed if the DV certificate permits access to DG 3 and DG 4 while the IS certificate enables only the access to DG 4.
Version	EAC2_1.0
Profile	ePassport, TA2_IS, DG3
Preconditions	<ol style="list-style-type: none"> 1. The PACE (MRZ) mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 3” chapter as DV_CERT_3 '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This DV-Certificate grants access to data group 3 and 4. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 3” chapter as IS_CERT_3b. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This IS-Certificate grants only access to data group 4. 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS-Certificate sent in step

	<p>4 has to be used.</p> <ol style="list-style-type: none"> 6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_03. 8. The Chip Authentication mechanism MUST be performed. 9. Send the given Select Application APDU to the eID Card (selecting ePassport application): '0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ePassport application-ID. 10. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 3 has NOT been granted. '0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. true 9. '90 00' within a valid Secure Messaging response. 10. Checking error

3.7.5 Test case EAC2_ISO7816_L_5

Test - ID	EAC2_ISO7816_L_5
Purpose	Positive test with a valid terminal authentication process for DG 3 if the DV certificate grant access to data group 3 only and the IS certificate enable access to both data 3 and 4.
Version	EAC2_1.0
Profile	ePassport, TA2_IS, DG3
Preconditions	<ol style="list-style-type: none"> 1. The PACE (MRZ) mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism.

	<p>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 4” chapter as DV_CERT_4 `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>’</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This DV-Certificate grants access to data group 3 only. <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00’</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS-Certificate as specified in the “Certificate Set 4” chapter as IS_CERT_4. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>’</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This IS-Certificate grants access to data group 3 and 4. <p>5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00’</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’</p> <p>7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>’</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_04. <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting ePassport application): `0C A4 04 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00’</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ePassport application-ID. <p>10. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 3 has been granted.</p>
--	---

	'0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. true 9. '90 00' within a valid Secure Messaging response. 10. '<first byte of data group 3 content data> 90 00' within a valid Secure Messaging response.

3.7.6 Test case EAC2_ISO7816_L_6

Test - ID	EAC2 ISO7816 L 6
Purpose	Test that data group 4 cannot be accessed if the DV certificate grant access to data group 3 only and the IS certificate enable access to both data 3 and 4.
Version	EAC2 1.0
Profile	ePassport, TA2_IS, DG4
Preconditions	<ol style="list-style-type: none"> 1. The PACE (MRZ) mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 4” chapter as DV_CERT_4 '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This DV-Certificate grants access to data group 3 only. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 4” chapter

	<p>as IS_CERT_4.</p> <p>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This IS-Certificate grants access to data group 3 and 4. <p>5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_04. <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting ePassport application): '0C A4 04 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ePassport application-ID. <p>10. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 4 has NOT been granted. '0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. true 9. '90 00' within a valid Secure Messaging response. 10. Checking error within a valid Secure Messaging response.

3.7.7 Test case EAC2_ISO7816_L_7

Test - ID	EAC2 ISO7816 L 7
-----------	------------------

Test plan for eID-Cards with EAC 2.0

Purpose	Positive test with a valid terminal authentication process for DG 4 if the DV certificate grant access to data group 4 only and the IS certificate enables access to both data 3 and 4.
Version	EAC2 1.0
Profile	ePassport, TA2 IS, DG4
Preconditions	<ol style="list-style-type: none"> 1. The PACE (MRZ) mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 5” chapter as DV_CERT_5 '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This DV-Certificate grants access to data group 4 only. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 5” chapter as IS_CERT_5. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This IS-Certificate grants access to data group 3 and 4. 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eID Card.

	<pre>'0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</pre> <p>7. Send the given external authenticate command to the eID Card. <code>'0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</code></p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_05. <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting ePassport application): <code>'0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</code></p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ePassport application-ID. <p>10. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 4 has been granted. <code>'0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00'</code></p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. true 9. '90 00' within a valid Secure Messaging response. 10. '<first byte of data group 4 content data> 90 00' within a valid Secure Messaging response.

3.7.8 Test case EAC2_ISO7816_L_8

Test - ID	EAC2_ISO7816_L_8
Purpose	Test that data group 3 cannot be accessed if the DV certificate grants access to data group 4 only and the IS certificate enables access to both data group 3 and 4.
Version	EAC2 1.0
Profile	ePassport, TA2_IS, DG3
Preconditions	<ol style="list-style-type: none"> 1. The PACE (MRZ) mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. <code>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</code> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects <code>83 <L₈₃> <Certification Authority Reference></code> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the "Certificate Set 5" chapter as DV_CERT_5

Test plan for eID-Cards with EAC 2.0

	<pre>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This DV-Certificate grants access to data group 4 only. <p>3. Send the given MSE: Set DST APDU to the eID Card. <pre>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS-Certificate as specified in the “Certificate Set 5” chapter as IS_CERT_5. <pre>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This IS-Certificate grants access to data group 3 and 4. <p>5. Send the given MSE: Set AT APDU to the eID Card. <pre>'0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. <pre>'0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</pre> <p>7. Send the given external authenticate command to the eID Card. <pre>'0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_05. <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting ePassport application): <pre>'0C A4 04 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ePassport application-ID. <p>10. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 3 has NOT been granted. <pre>'0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'</pre> </p> </p></p></p></p></p></p>
Expected results	<p>1. '90 00' within a valid Secure Messaging response.</p>

	<ol style="list-style-type: none"> 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. true 9. '90 00' within a valid Secure Messaging response. 10. Checking error within a valid Secure Messaging response.
--	--

3.7.9 Test case EAC2_ISO7816_L_9

Test - ID	EAC2 ISO7816 L 9
Purpose	This test verifies that a successful certificate chain validation without external authenticate does not enable the access to the sensitive data in data group 3.
Version	EAC2 1.0
Profile	ePassport, TA2_IS, DG3
Preconditions	<ol style="list-style-type: none"> 1. The PACE (MRZ) mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1 '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects

Test plan for eID-Cards with EAC 2.0

	<p>7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature></p> <p>5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. The Chip Authentication mechanism MUST be performed.</p> <p>8. Send the given Select Application APDU to the eID Card (selecting ePassport application): '0C A4 04 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ePassport application-ID. <p>9. If the previous step returned an error, skip this step. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 3 has NOT been granted. '0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. false 8. '90 00' or checking error within a valid Secure Messaging response. 9. Skipped or checking error within a valid Secure Messaging response.

3.7.10 Test case EAC2_ISO7816_L_10

Test - ID	EAC2_ISO7816_L_10
Purpose	This test verifies that a successful certificate chain validation without external authenticate does not enable the access to the sensitive data in data group 4
Version	EAC2_1.0
Profile	ePassport, TA2_IS, DG4
Preconditions	<ol style="list-style-type: none"> 1. The PACE (MRZ) mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'

	<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1 `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> <p>5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. The Chip Authentication mechanism MUST be performed.</p> <p>8. Send the given Select Application APDU to the eID Card (selecting ePassport application): `0C A4 04 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ePassport application-ID. <p>9. If the previous step returned an error, skip this step. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 4 has NOT been granted. `0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00'</p>
Expected results	1. '90 00' within a valid Secure Messaging response.

	<ol style="list-style-type: none"> 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. false 8. '90 00' or checking error within a valid Secure Messaging response. 9. Skipped or checking error within a valid Secure Messaging response.
--	---

3.7.11 Test case EAC2_ISO7816_L_11

Test - ID	EAC2_ISO7816_L_11
Purpose	Test with a failed external authenticate command does not enable the access to the sensitive data in data group 3.
Version	EAC2 1.0
Profile	ePassport, TA2_IS, DG3
Preconditions	<ol style="list-style-type: none"> 1. The PACE (MRZ) mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body>

	<p>5F 37 <L5F37> <certificate signature></p> <p>5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'></p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_01. • The last byte of the signature is changed to make it invalid <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting ePassport application): `0C A4 04 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ePassport application-ID. <p>10. If the previous step returned an error, skip this step. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 3 has NOT been granted. `0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. Checking error or warning processing '63 00' within a valid Secure Messaging response. 8. false 9. '90 00' or checking error within a valid Secure Messaging response. 10. Skipped or checking error within a valid Secure Messaging response

3.7.12 Test case EAC2_ISO7816_L_12

Test - ID	EAC2 ISO7816 L 12
Purpose	Test with a failed external authenticate command does not enable the access to the sensitive data in data group 4.

Test plan for eID-Cards with EAC 2.0

Version	EAC2 1.0
Profile	ePassport, TA2 IS, DG4
Preconditions	<ol style="list-style-type: none"> 1. The PACE (MRZ) mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 1” chapter as DV_CERT_1. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 1” chapter as IS_CERT_1. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference> 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created

	<p>with the private key of IS_KEY_01.</p> <ul style="list-style-type: none"> • The last byte of the signature is changed to make it invalid <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting ePassport application): '0C A4 04 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ePassport application-ID. <p>10. If the previous step returned an error, skip this step. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 4 has NOT been granted. '0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. Checking error or warning processing '63 00' within a valid Secure Messaging response. 8. false 9. '90 00' or checking error within a valid Secure Messaging response. 10. Skipped or checking error within a valid Secure Messaging response.

3.7.13 Test case EAC2_ISO7816_L_13 Template

Test - ID	EAC2 ISO7816 L 13 template
Purpose	Positive test with a valid terminal authentication process with read access permission for well defined DGs if the DV certificate permits read access to all DGs while the Terminal certificate restricts access to one DG. DV certificate is an official domestic certificate.
Version	See Table 63
Profile	SMARTeID or eID , TA2_AT, required data group presence see Table 63
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed (PIN). 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the "Certificate Set 19" chapter as DV_CERT_19. '0C 2A 00 BE <Lc> 87 <L87> 01 <Cryptogram> 8E 08

	<pre><Checksum> <Le>'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This DV-Certificate grants read access to all data groups. <p>3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate Terminal-Certificate as specified in the "Certificate Set 19" chapter as defined in Table 63, column Cert Reference '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This Terminal-Certificate grants access to data groups as defined in Table 63, column Access Rules. <p>5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference> 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting eID application): '0C A4 04 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted eID application-ID. <p>10. Send the given Read Binary (with SFI) command to the eID Card, to verify the read access to the selected data group has been granted. '0C B0 (80 <SFI>) 00 0D 97 01 01 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <SFI> contains the SFI reference as defined in Table 63, column <i>SFI</i>.
--	---

Expected results	<ol style="list-style-type: none">1. '90 00' within a valid Secure Messaging response.2. '90 00' within a valid Secure Messaging response.3. '90 00' within a valid Secure Messaging response.4. '90 00' within a valid Secure Messaging response.5. '90 00' within a valid Secure Messaging response.6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response.7. '90 00' within a valid Secure Messaging response.8. True9. '90 00' within a valid Secure Messaging response.10. '<first byte of data group content data> 90 00' within a valid Secure Messaging response.
------------------	--

Test case EAC2 ISO7816 L 13a to Test case EAC2 ISO7816 L 13v:

Test Case ID	Version	Access Rules	Cert Reference	SFI
EAC2 ISO7816 L 13a	EAC2 1.0	This terminal certificate grants only read access to data group 1	AT CERT_19a	0x01
EAC2 ISO7816 L 13b	EAC2 1.0	This terminal certificate grants only read access to data group 2	AT CERT_19b	0x02
EAC2 ISO7816 L 13c	EAC2 1.0	This terminal certificate grants only read access to data group 3	AT CERT_19c	0x03
EAC2 ISO7816 L 13d	EAC2 1.0	This terminal certificate grants only read access to data group 4	AT CERT_19d	0x04
EAC2 ISO7816 L 13e	EAC2 1.0	This terminal certificate grants only read access to data group 5	AT CERT_19e	0x05
EAC2 ISO7816 L 13f	EAC2 1.0	This terminal certificate grants only read access to data group 6	AT CERT_19f	0x06
EAC2 ISO7816 L 13g	EAC2 1.0	This terminal certificate grants only read access to data group 7	AT CERT_19g	0x07
EAC2 ISO7816 L 13h	EAC2 1.0	This terminal certificate grants only read access to data group 8	AT CERT_19h	0x08
EAC2 ISO7816 L 13i	EAC2 1.0	This terminal certificate grants only read access to data group 9	AT CERT_19i	0x09
EAC2 ISO7816 L 13j	EAC2 1.0	This terminal certificate grants only read access to data group 10	AT CERT_19j	0x0a
EAC2 ISO7816 L 13k	EAC2 1.0	This terminal certificate grants only read access to data group 11	AT CERT_19k	0x0b
EAC2 ISO7816 L 13l	EAC2 1.0	This terminal certificate grants only read access to data group 12	AT CERT_19l	0x0c
EAC2 ISO7816 L 13m	EAC2 1.0	This terminal certificate grants only read access to data group 13	AT CERT_19m	0x0d
EAC2 ISO7816 L 13n	EAC2 1.0	This terminal certificate grants only read access to data group 14	AT CERT_19n	0x0e
EAC2 ISO7816 L 13o	EAC2 1.0	This terminal certificate grants only read access to data group 15	AT CERT_19o	0x0f
EAC2 ISO7816 L 13p	EAC2 1.0	This terminal certificate grants only read access to data group 16	AT CERT_19p	0x10
EAC2 ISO7816 L 13q	EAC2 1.0	This terminal certificate grants only read access to data group 17	AT CERT_19q	0x11
EAC2 ISO7816 L 13r	EAC2 1.0	This terminal certificate grants only read access to data group 18	AT CERT_19r	0x12
EAC2 ISO7816 L 13s	EAC2 1.0	This terminal certificate grants only read access to data group 19	AT CERT_19s	0x13
EAC2 ISO7816 L 13t	EAC2 1.0	This terminal certificate grants only read access to data group 20	AT CERT_19t	0x14
EAC2 ISO7816 L 13u	EAC2 1.0	This terminal certificate grants only read access to data group 21	AT CERT_19u	0x15
EAC2 ISO7816 L 13v	EAC2 1.1	This terminal certificate grants only read access to data group 22	AT CERT_19v	0x16

Table 63: Test cases EAC2_ISO7816_L_13

3.7.14 Test case EAC2_ISO7816_L_14 Template

Test - ID	EAC2_ISO7816_L_14_template
Purpose	Positive test with a valid terminal authentication process with read access permission for well defined DGs if the DV certificate permits read access to all DGs while the Terminal certificate restricts access to one DG. DV certificate is a non-official certificate.
Version	See Table 64
Profile	SMARTeID or eID, TA2_AT, required data group presence see Table 64
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed (PIN). 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 20” chapter as DV_CERT_20. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This DV-Certificate grants read access to all data groups. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 20” chapter as defined in Table 64, column Cert Reference '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This Terminal-Certificate grants access to data groups as defined in Table 64, column Access Rules 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects

Test plan for eID-Cards with EAC 2.0

	<p>80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key></p> <ul style="list-style-type: none"> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting eID application): '0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted eID application-ID. <p>10. Send the given Read Binary (with SFI) command to the eID Card, to verify the read access to the selected data group has been granted. '0C B0 (80 <SFI>) 00 0D 97 01 01 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <SFI> contains the SFI reference as defined in Table 64, column <i>SFI</i>.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. True 9. '90 00' within a valid Secure Messaging response. 10. '<first byte of data group content data> 90 00' within a valid Secure Messaging response.

Test case EAC2 ISO7816 L 14a to Test case EAC2 ISO7816 L 14v

Test Case ID	Version	Access Rules	Cert Reference	SFI
EAC2 ISO7816 L 14a	EAC2 1.0	This terminal certificate grants only read access to data group 1	AT_CERT_20a	0x01
EAC2 ISO7816 L 14b	EAC2 1.0	This terminal certificate grants only read access to data group 2	AT_CERT_20b	0x02
EAC2 ISO7816 L 14c	EAC2 1.0	This terminal certificate grants only read access to data group 3	AT_CERT_20c	0x03
EAC2 ISO7816 L 14d	EAC2 1.0	This terminal certificate grants only read access to data group 4	AT_CERT_20d	0x04
EAC2 ISO7816 L 14e	EAC2 1.0	This terminal certificate grants only read access to data group 5	AT_CERT_20e	0x05
EAC2 ISO7816 L 14f	EAC2 1.0	This terminal certificate grants only read access to data group 6	AT_CERT_20f	0x06
EAC2 ISO7816 L 14g	EAC2 1.0	This terminal certificate grants only read access to data group 7	AT_CERT_20g	0x07
EAC2 ISO7816 L 14h	EAC2 1.0	This terminal certificate grants only read access to data group 8	AT_CERT_20h	0x08
EAC2 ISO7816 L 14i	EAC2 1.0	This terminal certificate grants only read access to data group 9	AT_CERT_20i	0x09
EAC2 ISO7816 L 14j	EAC2 1.0	This terminal certificate grants only read access to data group 10	AT_CERT_20j	0x0a
EAC2 ISO7816 L 14k	EAC2 1.0	This terminal certificate grants only read access to data group 11	AT_CERT_20k	0x0b
EAC2 ISO7816 L 14l	EAC2 1.0	This terminal certificate grants only read access to data group 12	AT_CERT_20l	0x0c
EAC2 ISO7816 L 14m	EAC2 1.0	This terminal certificate grants only read access to data group 13	AT_CERT_20m	0x0d
EAC2 ISO7816 L 14n	EAC2 1.0	This terminal certificate grants only read access to data group 14	AT_CERT_20n	0x0e
EAC2 ISO7816 L 14o	EAC2 1.0	This terminal certificate grants only read access to data group 15	AT_CERT_20o	0x0f
EAC2 ISO7816 L 14p	EAC2 1.0	This terminal certificate grants only read access to data group 16	AT_CERT_20p	0x10
EAC2 ISO7816 L 14q	EAC2 1.0	This terminal certificate grants only read access to data group 17	AT_CERT_20q	0x11
EAC2 ISO7816 L 14r	EAC2 1.0	This terminal certificate grants only read access to data group 18	AT_CERT_20r	0x12
EAC2 ISO7816 L 14s	EAC2 1.0	This terminal certificate grants only read access to data group 19	AT_CERT_20s	0x13
EAC2 ISO7816 L 14t	EAC2 1.0	This terminal certificate grants only read access to data group 20	AT_CERT_20t	0x14
EAC2 ISO7816 L 14u	EAC2 1.0	This terminal certificate grants only read access to data group 21	AT_CERT_20u	0x15
EAC2 ISO7816 L 14v	EAC2 1.1	This terminal certificate grants only read access to data group 22	AT_CERT_20v	0x16

Table 64: Test cases EAC2_ISO7816_L_14

3.7.15 Test case EAC2_ISO7816_L_15 Template

Test - ID	EAC2_ISO7816_L_15_template
Purpose	Positive test with a valid terminal authentication process with write access permission for well defined DGs if the DV certificate permits write access to all writable DGs while the Terminal certificate restricts access to one DG. DV certificate is an official domestic certificate
Version	See Table 65
Profile	eID, TA2_AT, required data group presence see Table 65
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed (PIN). 2. All APDUs are sent as valid SecureMessaging APDUs. 3. Read content of DG 17 to DG 22 to restore the content after this test scenario using DV_CERT_19 and AT_CERT_19q to AT_CERT_19v
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 21” chapter as DV_CERT_21. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This DV-Certificate grants write access to all writable data groups. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L83> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 21” chapter as referenced in Table 65, column Cert Reference '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L7F4E> <certificate body> 5F 37 <L5F37> <certificate signature> • This Terminal-Certificate grants access to data groups as defined in Table 65, column Access Rules. 5. Send the given MSE: Set AT APDU to the eID Card.

	<pre>'0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L80> <Cryptographic Mechanism Reference> 83 <L83> <Certificate Holder Reference > 91 <L91> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. <pre>'0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</pre></p> <p>7. Send the given external authenticate command to the eID Card. <pre>'0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting eID application): <pre>'0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted eID application-ID. <p>10. Send the given Update Binary (with SFI) command to the eID Card, to verify that write access to the selected data group has been granted. <pre>'0C D6 (80 <SFI>) 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: 01 02 03 04 • <SFI> contains the SFI reference as defined in Table 65, column SFI. </p> </p></p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. True 9. '90 00' within a valid Secure Messaging response. 10. '90 00' within a valid Secure Messaging response.
Post processing	1. Restore original content of DG 17 to DG 22

Test case EAC2_ISO7816_L_15a to Test case EAC2_ISO7815_L_15f:

Test Case ID	Version	Access Rules	Cert Reference	SFI
EAC2_ISO7816_L_15a	EAC2_1.0 3	This terminal certificate grants only r/w access to data group 17	AT_CERT_21a	0x11
EAC2_ISO7816_L_15b	EAC2_1.0 3	This terminal certificate grants only r/w access to data group 18	AT_CERT_21b	0x12

Test Case ID	Version	Access Rules	Cert Reference	SFI
EAC2_ISO7816_L_15c	EAC2_1.0 3	This terminal certificate grants only r/w access to data group 19	AT_CERT_21c	0x13
EAC2_ISO7816_L_15d	EAC2_1.0 3	This terminal certificate grants only r/w access to data group 20	AT_CERT_21d	0x14
EAC2_ISO7816_L_15e	EAC2_1.0 3	This terminal certificate grants only r/w access to data group 21	AT_CERT_21e	0x15
EAC2_ISO7816_L_15f	EAC2_1.1	This terminal certificate grants only r/w access to data group 22	AT_CERT_21f	0x16

Table 65: Test cases EAC2_ISO7816_L_15**3.7.16 Test case EAC2_ISO7816_L_16 Template**

Test - ID	EAC2_ISO7816_L_16_template
Purpose	Positive test with a valid terminal authentication process with write access permission for well defined DGs if the DV certificate permits write access to all writable DGs while the Terminal certificate restricts access to one DG. DV certificate is a non-official certificate
Version	See Table 66
Profile	eID, TA2_AT, required data group presence see Table 66
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed (PIN). All APDUs are sent as valid SecureMessaging APDUs. Read content of DG 17 to DG 22 to restore the content after this test scenario using DV_CERT_19 and AT_CERT_19q to AT_CERT_19v
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certification Authority Reference MUST be used as returned by the PACE mechanism. Send the appropriate DV-Certificate as specified in the “Certificate Set 22” chapter as DV_CERT_22. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This DV-Certificate grants write access to all writable data groups. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certificate Holder Reference stored inside the DV-Certificate sent in

	<p>step 2 has to be used.</p> <p>4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 22” chapter as defined in Table 66, column Cert Reference. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants only write access to data groups as defined in Table 66, column Access Rules. <p>5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference > 91 <L₉₁> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting eID application): `00 A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature <p>10. Send the given Update Binary (with SFI) command to the eID Card, to verify that write access to the selected data group has been granted. `0C D6 (80 <SFI>) 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: 01 02 03 04 • <SFI> contains the SFI reference as defined in Table 66, column SFI </p> </p></p></p></p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. True

Test plan for eID-Cards with EAC 2.0

	9. '90 00' within a valid Secure Messaging response. 10. '90 00' within a valid Secure Messaging response.
Post processing	1. Restore original content of DG 17 to DG 22

Test case EAC2_ISO7816_L_16a to Test case EAC2_ISO7816_L_16e:

Test Case ID	Version	Access Rules	Cert Reference	SFI
EAC2_ISO7816_L_16a	EAC2_1.0 3	This terminal certificate grants only r/w access to data group 17	AT_CERT_22a	0x11
EAC2_ISO7816_L_16b	EAC2_1.0 3	This terminal certificate grants only r/w access to data group 18	AT_CERT_22b	0x12
EAC2_ISO7816_L_16c	EAC2_1.0 3	This terminal certificate grants only r/w access to data group 19	AT_CERT_22c	0x13
EAC2_ISO7816_L_16d	EAC2_1.0 3	This terminal certificate grants only r/w access to data group 20	AT_CERT_22d	0x14
EAC2_ISO7816_L_16e	EAC2_1.0 3	This terminal certificate grants only r/w access to data group 21	AT_CERT_22e	0x15
EAC2_ISO7816_L_16f	EAC2_1.1	This terminal certificate grants only r/w access to data group 22	AT_CERT_22f	0x16

Table 66: Test cases EAC2_ISO7816_L_16

3.7.17 Test case EAC2_ISO7816_L_17

Test - ID	EAC2_ISO7816_L_17
Purpose	Positive test with a valid terminal authentication process with rights for special functions if the DV certificate permits all special functions while the terminal certificate restricts access to one special function. DV certificate is an official domestic certificate. Special function allowed by terminal certificate is Age Verification. Date of birth must be specified in ICS.
Version	EAC2_1.0
Profile	eID or SMARTeID, TA2_AT
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed (PIN). All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certification Authority Reference MUST be used as returned by the PACE mechanism. Send the appropriate DV-Certificate as specified in the "Certificate Set 17" chapter as DV_CERT_17. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This DV-Certificate grants access to all eID special functions. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08

	<pre><Checksum> 00' • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 17” chapter as AT_CERT_17f. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to special function “Age Verification” 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference > 91 <L₉₁> <Compressed Ephemeral Public Key> 67 <L₆₇> <Auxiliary Data> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. • Auxiliary Data contains valid Date of Birth data as specified in ICS. 6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the encrypted terminal generated signature 8. The Chip Authentication mechanism MUST be performed. 9. Send the given Select Application APDU to the eID Card (selecting eID application): '0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the encrypted eID application-ID. 10. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth></pre>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response.

	<p>5. '90 00' within a valid Secure Messaging response.</p> <p>6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response.</p> <p>7. '90 00' within a valid Secure Messaging response.</p> <p>8. True</p> <p>9. '90 00' within a valid Secure Messaging response.</p> <p>10. '90 00' within a valid Secure Messaging response.</p>
--	--

3.7.18 Test case EAC2_ISO7816_L_18

Test - ID	EAC2_ISO7816_L_18
Purpose	Test with a valid terminal authentication process with rights for special functions if the DV certificate permits all special functions while the terminal certificate restricts access to one special function. DV certificate is an official domestic certificate. Special function allowed by terminal certificate is "Install Qualified Certificate" but "Age Verification" is used. Date of birth must be specified in ICS.
Version	EAC2 1.0
Profile	eID or SMARTeID, TA2 AT
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed (PIN). All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certification Authority Reference MUST be used as returned by the PACE mechanism. Send the appropriate DV-Certificate as specified in the "Certificate Set 17" chapter as DV_CERT_17. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This DV-Certificate grants access to all eID special functions. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. Send the appropriate Terminal-Certificate as specified in the "Certificate Set 17" chapter as AT_CERT_17d. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'

Test plan for eID-Cards with EAC 2.0

	<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to special function “Install Qualified Certificate” <p>5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference > 91 <L₉₁> <Compressed Ephemeral Public Key> 67 <L₆₇> <Auxiliary Data> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. • Auxiliary Data contains valid Date of Birth data as specified in ICS. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting eID application): '0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted eID application-ID. <p>10. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. True 9. '90 00' within a valid Secure Messaging response. 10. '69 82' within a valid Secure Messaging response.

3.7.19 Test case EAC2_ISO7816_L_19

Test - ID	EAC2 ISO7816 L 19
Purpose	Positive test with a valid terminal authentication process with rights for special functions if the DV certificate permits all special functions while the terminal certificate restricts access to one special function. DV certificate is an official domestic certificate. Special function allowed by terminal certificate is Municipality ID Verification.
Version	EAC2 1.03
Profile	SMARTeID or eID, TA2 AT
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed (PIN). 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 17” chapter as DV_CERT_17. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to all eID special functions. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 17” chapter as AT_CERT_17g. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to special function “Municipality ID Verification” 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference>

Test plan for eID-Cards with EAC 2.0

	<p>83 <L₈₃> <Certificate Holder Reference > 91 <L₉₁> <Compressed Ephemeral Public Key> 67 <L₆₇> <Auxiliary Data></p> <ul style="list-style-type: none"> The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. Auxiliary Data contains valid Municipality ID data. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the encrypted terminal generated signature</p> <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting eID application): '0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the encrypted eID application-ID.</p> <p>10. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-MunicipalityID></p>
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. '90 00' within a valid Secure Messaging response. True '90 00' within a valid Secure Messaging response. '90 00' within a valid Secure Messaging response.

3.7.20 Test case EAC2_ISO7816_L_20

Test - ID	EAC2_ISO7816_L_20
Purpose	Test with a valid terminal authentication process with rights for special functions if the DV certificate permits all special functions while the terminal certificate restricts access to one special function. DV certificate is an official domestic certificate. Special function allowed by terminal certificate is "Install Qualified Certificate" but "Municipality ID Verification" is used.
Version	EAC2_1.0
Profile	SMARTeID or eID, TA2_AT
Preconditions	1. The PACE mechanism MUST have been performed (PIN).

	<p>2. All APDUs are sent as valid SecureMessaging APDUs.</p>
Test scenario	<p>1. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 17” chapter as DV_CERT_17. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to all eID special functions. <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 17” chapter as AT_CERT_17d. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to special function “Install Qualified Certificate” <p>5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference > 91 <L₉₁> <Compressed Ephemeral Public Key> 67 <L₆₇> <Auxiliary Data> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. • Auxiliary Data contains valid Municipality ID data. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08</p>

Test plan for eID-Cards with EAC 2.0

	<p><Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting eID application):</p> <p>'0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted eID application-ID. <p>10. Send the given Verify APDU to the eID Card.</p> <p>'8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: <id-MunicipalityID>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. True 9. '90 00' within a valid Secure Messaging response. 10. '69 82'. The error MUST be encoded in a valid Secure Messaging response.

3.7.21 Test case EAC2_ISO7816_L_21

Test - ID	EAC2_ISO7816_L_21
Version	deleted in version 1.00 RC

3.7.22 Test case EAC2_ISO7816_L_22

Test - ID	EAC2_ISO7816_L_22
Version	deleted in version 1.00 RC

3.7.23 Test case EAC2_ISO7816_L_23

Test - ID	EAC2_ISO7816_L_23
Purpose	Positive test with a valid terminal authentication process with rights for special functions if the DV certificate permits all special functions while the terminal certificate restricts access to one special function. DV certificate is an official domestic certificate. Special function allowed by terminal certificate is "CAN allowed".
Version	EAC2_1.0
Profile	eID, TA2_AT
Preconditions	1. The PACE mechanism MUST have been performed (using CAN).

	<p>2. All APDUs are sent as valid SecureMessaging APDUs.</p>
Test scenario	<p>1. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 17” chapter as DV_CERT_17. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to all eID special functions. <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 17” chapter as AT_CERT_17a. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to special function “CAN allowed” <p>5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> 91 <L₉₁> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p>

	<p>9. Send the given Select Application APDU to the eID Card (selecting eID application): `0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <p>10. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 1 has been granted. `0C B0 81 00 0D 97 01 01 8E 08 <Checksum> 00'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. True 9. '90 00' within a valid Secure Messaging response. 10. '90 00' within a valid Secure Messaging response.

3.7.24 Test case EAC2_ISO7816_L_24

Test - ID	EAC2_ISO7816_L_24
Version	deleted in version 1.00 RC

3.7.25 Test case EAC2_ISO7816_L_25

Test - ID	EAC2_ISO7816_L_25
Purpose	Positive test with a valid terminal authentication process with rights for special functions if the DV certificate permits all special functions while the terminal certificate restricts access to one special function. DV certificate is an official domestic certificate. Special function allowed by terminal certificate is “PIN Management”. Deactivate PIN within pin management is tested.
Version	EAC2_1.0
Profile	eID, TA2_AT
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed (using PIN). 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<p>1. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 17” chapter as DV_CERT_17. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08</p>

	<p><Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to all eID special functions. <p>3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate Terminal-Certificate as specified in the "Certificate Set 17" chapter as AT_CERT_17b. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to special function "PIN Management" <p>5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> 91 <L₉₁> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Deactivate PIN APDU to the eID Card: '0C 04 10 03 <Lc> 8E 08 <Checksum> 00'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response.

	<ul style="list-style-type: none"> 8. True 9. '90 00' within a valid Secure Messaging response.
--	---

3.7.26 Test case EAC2_ISO7816_L_26

Test - ID	EAC2_ISO7816_L_26
Purpose	Positive test with a valid terminal authentication process with rights for special functions if the DV certificate permits all special functions while the terminal certificate restricts access to one special function. DV certificate is an official domestic certificate. Special function allowed by terminal certificate is “PIN Management”. Activate PIN within pin management is tested.
Version	EAC2 1.0
Profile	eID, TA2_AT
Preconditions	<ul style="list-style-type: none"> 1. PIN MUST have been deactivated (see Test case EAC2_ISO7816_L_25). 2. The PACE mechanism MUST have been performed (using CAN). 3. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ul style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 17” chapter as DV_CERT_17. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to all eID special functions. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 17” chapter as AT_CERT_17b. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to special function “PIN

	<p>Management”</p> <ol style="list-style-type: none"> 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> 91 <L₉₁> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature 8. The Chip Authentication mechanism MUST be performed. 9. Send the given Activate PIN APDU to the eID Card: '0C 44 10 03 <Lc> 8E 08 <Checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. True 9. '90 00' within a valid Secure Messaging response.

3.7.27 Test case EAC2_ISO7816_L_27

Test - ID	EAC2_ISO7816_L_27
Purpose	Test with a valid terminal authentication process with rights for special functions if the DV certificate permits all special functions while the terminal certificate restricts access to one special function. DV certificate is an official domestic certificate. Special function allowed by terminal certificate is “Install Qualified Certificate” but “PIN Management” is used.
Version	EAC2 1.0
Profile	eID, TA2_AT
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed (using PIN). 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects

	<p>83 <L₈₃> <Certification Authority Reference></p> <ul style="list-style-type: none"> The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 17” chapter as DV_CERT_17. ‘0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>’</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This DV-Certificate grants access to all eID special functions. <p>3. Send the given MSE: Set DST APDU to the eID Card. ‘0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00’</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 17” chapter as AT_CERT_17d. ‘0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>’</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This Terminal-Certificate grants access to special function “Install Qualified Certificate” <p>5. Send the given MSE: Set AT APDU to the eID Card. ‘0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00’</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> 91 <L₉₁> <Compressed Ephemeral Public Key> The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. ‘0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’</p> <p>7. Send the given external authenticate command to the eID Card. ‘0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00’</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Deactivate PIN APDU to the eID Card: ‘0C 04 10 03 <Lc> 8E 08 <Checksum> 00’</p>
Expected results	<ol style="list-style-type: none"> ‘90 00’ within a valid Secure Messaging response. ‘90 00’ within a valid Secure Messaging response.

	<ol style="list-style-type: none"> 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. True 9. '69 82'. The error MUST be encoded in a valid Secure Messaging response.
--	---

3.7.28 Test case EAC2_ISO7816_L_28

Test - ID	EAC2_ISO7816_L_28
Purpose	Test with a valid terminal authentication process with rights for special functions if the DV certificate permits all special functions while the terminal certificate restricts access to one special function. DV certificate is an official domestic certificate. Special function allowed by terminal certificate is "Install Qualified Certificate" but "PIN Management" is used.
Version	EAC2_1.0
Profile	eID, TA2_AT
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed (using PIN). 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the "Certificate Set 17" chapter as DV_CERT_17. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to all eID special functions. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the "Certificate Set 17" chapter as AT_CERT_17d. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'

	<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This Terminal-Certificate grants access to special function “Install Qualified Certificate” <p>5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> 91 <L₉₁> <Compressed Ephemeral Public Key> The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Deactivate PIN APDU to the eID Card: '0C 04 10 03 <Lc> 8E 08 <Checksum> 00'</p>
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. '90 00' within a valid Secure Messaging response. True '69 82'. The error MUST be encoded in a valid Secure Messaging response.

3.7.29 Test case EAC2_ISO7816_L_29

Deleted in version 1.1

3.7.30 Test case EAC2_ISO7816_L_30

Deleted in version 1.1

3.7.31 Test case EAC2_ISO7816_L_31

Deleted in version 1.1

3.7.32 Test case EAC2_ISO7816_L_32

Deleted in version 1.1

3.7.33 Test case EAC2_ISO7816_L_33

Deleted in version 1.1

3.7.34 Test case EAC2_ISO7816_L_34

Deleted in version 1.1

3.7.35 Test case EAC2_ISO7816_L_35

Test - ID	EAC2 ISO7816 L 35
Purpose	Positive test with a valid terminal authentication process with access permission for DG 3 if the DV certificate permits access to DG 3 and DG 4 while the IS certificate enables only the access to DG 3. It is tested that RFU bits are ignored.
Version	EAC2_1.0
Profile	ePassport, TA2_IS, DG3
Preconditions	<ol style="list-style-type: none"> 1. The PACE (MRZ) mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 3” chapter as DV_CERT_3a. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to data group 3 and 4 and has all RFU bits set to 1. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 3” chapter

Test plan for eID-Cards with EAC 2.0

	<p>as IS_CERT_3c.</p> <p>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This IS-Certificate grants only access to data group 3 and has all RFU bits set to 1. <p>5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference > 91 <L₉₁> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_03. <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting ePassport application): '0C A4 04 0C <Lc> 87 <L87> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ePassport application-ID. <p>10. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 3 has been granted. '0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. true 9. '90 00' within a valid Secure Messaging response. 10. '<first byte of data group 3 content data> 90 00' within a valid Secure Messaging response.

3.7.36 Test case EAC2_ISO7816_L_36

Test - ID	EAC2 ISO7816 L 36
Purpose	Positive test with a valid terminal authentication process with read access permission for DG 1 if the DV certificate permits read access to all DGs while the terminal certificate restricts access to DG 1. DV certificate is an official domestic certificate. It is tested that RFU bit 31 (Authorization of Authentication Terminals) is ignored.
Version	EAC2 1.0
Profile	eID, TA2_IS, DG1
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed (CAN). 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 19” chapter as DV_CERT_19a. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants read access to all data groups and has all RFU bits set to 1. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 19” chapter as AT_CERT_19w. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to data group 1 and has all RFU bits set to 1. 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects

Test plan for eID-Cards with EAC 2.0

	<p>80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> 91 <L₉₁> <Compressed Ephemeral Public Key></p> <ul style="list-style-type: none"> The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting eID application): '0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted eID application-ID. <p>10. Send the given Read Binary (with SFI) command to the eID Card, to verify the read access to the selected data group has been granted. '0C B0 81 00 0D 97 01 01 8E 08 <Checksum> 00'</p>
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. '90 00' within a valid Secure Messaging response. True '90 00' within a valid Secure Messaging response. '<first byte of data group content data> 90 00' within a valid Secure Messaging response.

3.7.37 Test case EAC2_ISO7816_L_37

Test - ID	EAC2 ISO7816 L 37
Purpose	Positive test with a valid terminal authentication process. The DV certificate permits all special functions while the terminal certificate restricts access to one special function. The DV certificate is an official domestic certificate. The special function allowed by terminal certificate is "Privileged Terminal".
Version	EAC2 1.1
Profile	eID, TA2_IS, CS
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed (CAN). All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08

	<pre><Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 17” chapter as DV_CERT_17. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to all eID special functions. <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 17” chapter as AT_CERT_17h. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to special function “Privileged Terminal” <p>5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> 91 <L₉₁> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature <p>8. Send the given Read Binary (with SFI) command to the eID Card, to verify the read access to the selected data group has been granted. `0C B0 (80 <sfi.EF.ChipSecurity> 00 0D 97 01 01 8E</p>
--	--

	08 <Checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. '<One byte content of EF.ChipSecurity> 90 00' within a valid Secure Messaging response.

3.7.38 Test case EAC2_ISO7816_L_38

Test - ID	EAC2_ISO7816_L_38
Purpose	Positive test with a valid terminal authentication process. The DV certificate and the terminal certificate grant access to a eID access function that is reserved for future use (RFU). The eID MUST tolerate this certificate with a RFU bit.
Version	EAC2 1.2
Profile	SMARTeID or eID, TA2_AT, AUTH_EXT
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed (PIN). 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the "Certificate_Set_32" chapter as DV_CERT_32a. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to a RFU function. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the "Certificate_Set_32" chapter as AT_CERT_32a.

	<pre>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to a RFU function <p>5. Send the given MSE: Set AT APDU to the eID Card. <pre>'0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> 91 <L₉₁> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. <pre>'0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</pre> <p>7. Send the given external authenticate command to the eID Card. <pre>'0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature </p> </p></p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response.

3.7.39 Test case EAC2_ISO7816_L_39

Test - ID	EAC2_ISO7816_L_39
Purpose	Positive test with a valid terminal authentication process. The DV certificate and the terminal certificate grant access to a eID special function that is reserved for future use (RFU). The eID MUST tolerate this certificate with a RFU bit.
Version	EAC2 1.2
Profile	SMARTeID or eID, TA2_AT, AUTH_EXT
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed (PIN). 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. <pre>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects

	<p>83 <L₈₃> <Certification Authority Reference></p> <ul style="list-style-type: none"> The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>2. Send the appropriate DV-Certificate as specified in the “Certificate_Set_32” chapter as DV_CERT_32b. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This DV-Certificate grants access to a RFU function. <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate Terminal-Certificate as specified in the “Certificate_Set_32” chapter as AT_CERT_32b. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This Terminal-Certificate grants access to a RFU function <p>5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> 91 <L₉₁> <Compressed Ephemeral Public Key> The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response.

	<p>5. '90 00' within a valid Secure Messaging response.</p> <p>6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response.</p> <p>7. '90 00' within a valid Secure Messaging response.</p>
--	--

3.7.40 Test case EAC2_ISO7816_L_40

Test - ID	EAC2 ISO7816 L 40
Purpose	Positive test with a valid terminal authentication process. The DV certificate and the terminal certificate contain a certificate extension (authentication terminals) extended by two empty bytes. The authorization extension in both certificates are extended with leading '00 00' (56 bit instead of 40 bit). The eID MUST tolerate this certificate with extended extension.
Version	EAC2 1.2
Profile	SMARTeID or eID, TA2_AT, AUTH_EXT
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed (PIN). All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certification Authority Reference MUST be used as returned by the PACE mechanism. Send the appropriate DV-Certificate as specified in the "Certificate_Set_32" chapter as DV_CERT_32c. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This DV-Certificate contains an extended certificate extension. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. Send the appropriate Terminal-Certificate as specified in the "Certificate_Set_32" chapter as AT_CERT_32c '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>

	<ul style="list-style-type: none"> This Terminal-Certificate contains an extended certificate extension. <p>5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> 91 <L₉₁> <Compressed Ephemeral Public Key> The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. '90 00' within a valid Secure Messaging response.

3.7.41 Test case EAC2_ISO7816_L_41

Test - ID	EAC2_ISO7816_L_41
Purpose	Positive test with a valid terminal authentication process. The DV certificate and the terminal certificate contain a certificate extension (eID functions) extended by two empty bytes. The eID MUST tolerate this certificate with extended extension.
Version	EAC2_1.2
Profile	SMARTeID or eID, TA2_AT, AUTH_EXT
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed (PIN). All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certification Authority Reference MUST be used as returned by the PACE mechanism. Send the appropriate DV-Certificate as specified in the "Certificate_Set_32" chapter as DV_CERT_32d

	<pre>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate contains an extended certificate extension. <p>3. Send the given MSE: Set DST APDU to the eID Card. <pre>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate Terminal-Certificate as specified in the “Certificate_Set_32” chapter as AT_CERT_32d <pre>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate contains an extended certificate extension. <p>5. Send the given MSE: Set AT APDU to the eID Card. <pre>'0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> 91 <L₉₁> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. <pre>'0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</pre> <p>7. Send the given external authenticate command to the eID Card. <pre>'0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature </p></p></p></p></p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response.

3.7.42 Test case EAC2_ISO7816_L_42

Test - ID	EAC2 ISO7816 L 42
Purpose	Positive test with a valid terminal authentication process. The DV certificate and the terminal certificate contain a certificate extension (special functions) extended by two empty bytes. The eID MUST tolerate this certificate with extended extension.
Version	EAC2 1.2
Profile	SMARTeID or eID, TA2 AT, AUTH_EXT
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed (PIN). 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate_Set_32” chapter as DV_CERT_32e '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate contains an extended certificate extension. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the “Certificate_Set_32” chapter as AT_CERT_32e '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate contains an extended certificate extension. 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> 91 <L₉₁> <Compressed Ephemeral Public Key>

	<ul style="list-style-type: none"> The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. '90 00' within a valid Secure Messaging response.

3.7.43 Test case EAC2 ISO7816 L_43

Test - ID	EAC2 ISO7816 L_43
Purpose	Positive test with a valid terminal authentication process. The DV certificate and the terminal certificate contain an unknown OID in CHA. The eID MUST tolerate this certificate with unknown OID
Version	EAC2 1.2
Profile	SMARTeID or eID, TA2_AT, AUTH_EXT
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed (PIN). All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certification Authority Reference MUST be used as returned by the PACE mechanism. Send the appropriate DV-Certificate as specified in the "Certificate_Set_32" chapter as DV_CERT_32f `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This DV-Certificate contains an unknown OID. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08

Test plan for eID-Cards with EAC 2.0

	<p><Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate Terminal-Certificate as specified in the "Certificate_Set_32" chapter as AT_CERT_32f '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate contains an unknown OID. <p>5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> 91 <L₉₁> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response.

3.7.44 Test case EAC2_ISO7816_L_44

Test - ID	EAC2 ISO7816 L 44
Purpose	Positive test with a valid terminal authentication process. The DV certificate and the terminal certificate contain an unknown authorization extension OID in for eID access. The eID MUST tolerate this certificate with unknown OID
Version	EAC2 1.2

Profile	SMARTeID or eID, TA2_AT, AUTH_EXT
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed (PIN). 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate_Set_32” chapter as DV_CERT_32g '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate contains an unknown OID. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the “Certificate_Set_32” chapter as AT_CERT_32g '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate contains an unknown OID. 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> 91 <L₉₁> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. 6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'

	<ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response.

3.7.45 Test case EAC2_ISO7816_L_45

Test - ID	EAC2 ISO7816 L 45
Purpose	Positive test with a valid terminal authentication process. The DV certificate and the terminal certificate contain an unknown authorization extension OID in for special functions. The eID MUST tolerate this certificate with unknown OID
Version	EAC2 1.2
Profile	SMARTeID or eID, TA2_AT, AUTH_EXT
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed (PIN). 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the "Certificate_Set_32" chapter as DV_CERT_32h '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate contains an unknown OID. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the "Certificate_Set_32" chapter as AT_CERT_32h

	<pre>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate contains an unknown OID. <p>5. Send the given MSE: Set AT APDU to the eID Card. <pre>'0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> 91 <L₉₁> <Compressed Ephemeral Public Key> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. <pre>'0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</pre> <p>7. Send the given external authenticate command to the eID Card. <pre>'0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature </p> </p></p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response.

3.8 Unit EAC2_ISO7816_M Update mechanism

This unit contains all test cases, which update the chip's persistent memory. Therefore these tests can be performed only once with a combination of a distinct sample and set of certificates. To reproduce this test unit, a new set with future certificate dates has to be created or a different test object has to be used. Also, this unit should be performed from first to last test case in the given order.

The following diagram shows the movement of the chip's current date (arrow at top) and the trust points (bars) for ePassport and eID (moved by link certificates). Note: Test cases M_6 and M_8 do not change the chip's persistent memory.

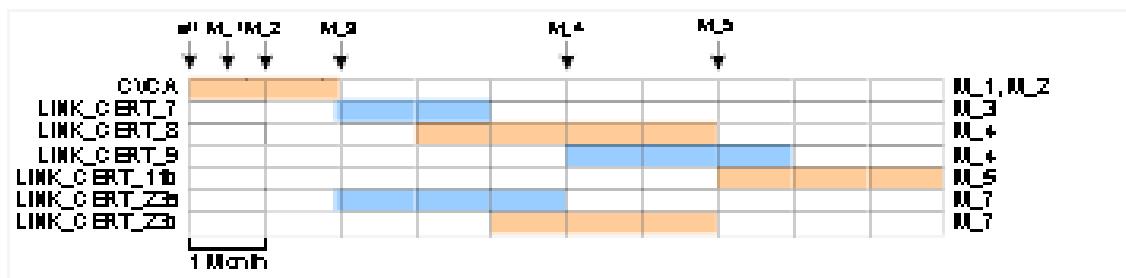


Figure 2: Test unit M overview

3.8.1 Test case EAC2_ISO7816_M_1_Template

Test - ID	EAC2 ISO7816 M 1 Template
Purpose	Test the “Current Date” update mechanism with a new certificate. This test works with IS/AT trust points.
Version	see table 67
Profile	see table 67
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed using password specified in table 67. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certification Authority Reference MUST be used as returned by the PACE mechanism. Send the appropriate DV-Certificate as specified in table 67 '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> The DV certificate is marked as a domestic certificate Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. Send the appropriate IS/AT-Certificate 1 as specified in table 67. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body>

	<p>5F 37 <L_{5F37}> <certificate signature></p> <ul style="list-style-type: none"> This certificate has an advanced effective date. Since the DV certificate was marked as a domestic one, the chip MUST update the current date. Reset the chip after this step and restore the preconditions for this test case before the next step is performed. <p>5. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>6. Send the appropriate DV-Certificate as specified in table 67. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> The DV certificate is marked as a domestic certificate <p>7. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certificate Holder Reference stored inside the DV-Certificate sent in step 6 has to be used. <p>8. Send the appropriate IS/AT-Certificate 2 as specified in table 67. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This certificate has an expiry date BEFORE the effective of the IS/AT certificate used in step 4. Therefore this certificate MUST be rejected.
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response. Checking error or '6300' within a valid Secure Messaging response. This certificate MUST no longer be valid, since the current date of the chip has been updated.

Test Case ID	Version	Profile	Certificates	Password
EAC2_ISO7816_M_1a	EAC2_1.0	TA2_IS	DV Cert: DV_CERT_6 Cert 1: IS_CERT_6a Cert 2: IS_CERT_6b	MRZ/CAN
EAC2_ISO7816_M_1b	Smart-eID	TA2_AT	DV Cert: DV_CERT_6b Cert 1: AT_CERT_6c Cert 2: AT_CERT_6d	PIN

Table 67: Test cases EAC2_ISO7816_M_1

3.8.2 Test case EAC2_ISO7816_M_2_Template

Test - ID	EAC2_ISO7816_M_2_Template
Purpose	Test the “Current Date” update mechanism with a new DV certificate. This test works with trust points.
Version	see table 68
Profile	see table 68
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed using password specified in table 68. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certification Authority Reference MUST be used as returned by the PACE mechanism. Send the appropriate DV-Certificate 1 as specified in table 68. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>, <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> The DV certificate has an advanced effective date beyond the expiration date of DV Cert 2 in table 68. Reset the chip after this step and restore the preconditions for this test case before the next step is performed. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certification Authority Reference MUST be used as returned by the PACE mechanism. Send the appropriate DV-Certificate 2 as specified in table 68

	<p>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This certificate has an expiration date before the effective date that was set in step 2. Therefore, this certificate SHALL be rejected
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. Checking error or '6300' within a valid Secure Messaging response. This certificate MUST no longer be valid, since the current date of the chip has been updated.

Test Case ID	Version	Profile	Certificates	Password
EAC2_ISO7816_M_2a	EAC2_1.0	TA2_IS	DV Cert 1: DV_CERT_6a DV Cert 2: DV_CERT_6	MRZ/CAN
EAC2_ISO7816_M_2b	Smart-eID	TA2_AT	DV Cert 1: DV_CERT_6c DV Cert 2: DV_CERT_6b	PIN

Table 68: Test cases EAC2_ISO7816_M_2

3.8.3 Test case EAC2_ISO7816_M_3_Template

Test - ID	EAC2_ISO7816_M_3_Template
Purpose	Test the “Trust Point” update mechanism with a new link certificate. This test changes the trust points.
Version	see table 69
Profile	see table 69
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using a password specified in table 69. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate link certificate as specified in table 69. The PICC MUST update the trust point with this new certificate. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects

	<p>7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature></p> <ol style="list-style-type: none"> 3. Power down the field or remove the passport from the reader, so that the chip loses all temporary information. This is done to prove, that the new trust point has been stored in persistent memory. Power up the chip again and perform PACE again and verify that the new trust point is at the first position (i.e. DO87) and the previous one has been moved to the second position (i.e. DO88). 4. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be the trust point received in DO 88 as returned by the PACE mechanism. 5. Send the appropriate DV-Certificate 1 as specified in table 69. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • Since the previous trust point is still valid, the certificate MUST be verified successfully. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 6. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be the trust point received in DO 87 as returned by the PACE mechanism. 7. Send the appropriate DV-Certificate 2 as specified in table 69. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • Since the effective date of this certificate is after the expiration date of the original trust point, the chip MUST update the current date and MUST also disable the original trust point for DV certificate verification. • Reset the chip after this step and restore the preconditions for this test case before the next step is performed. 8. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference>
--	---

	<ul style="list-style-type: none"> • Use the original Certification Authority Reference (same as in step 4). <p>9. Send the appropriate DV-Certificate 1 as specified in table 69. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • Since the trust point has been disabled for DV certificate verification, the certificate verification MUST fail.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. true 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. '90 00' or checking error within a valid Secure Messaging response. 9. Checking error or '6300' within a valid Secure Messaging response.. This certificate MUST no longer be valid, since the current date of the chip has been updated.

Test Case ID	Version	Profile	Certificates	Password
EAC2_ISO7816_M_3a	EAC2_1.0	TA2_IS	Link Cert: LINK_CERT_7 DV Cert 1: DV_CERT_7a DV Cert 2: DV_CERT_7b	MRZ/CAN
EAC2_ISO7816_M_3b	Smart-eID	TA2_AT	Link Cert: LINK_CERT_7a DV Cert 1: DV_CERT_7c DV Cert 2: DV_CERT_7d	PIN

Table 69: Test cases EAC2_ISO7816_M_3

3.8.4 Test case EAC2_ISO7816_M_4_Template

Before performing this test case, validate, that the trust point has successfully been updated in test case EAC2_ISO7816_M_3.

Test - ID	EAC2_ISO7816_M_4_Template
Purpose	Test the “Trust Point” update mechanism with two link certificates. This test changes the trust points.
Version	see table 70
Profile	see table 70
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using password specified in table 70.

	<ol style="list-style-type: none"> 2. All APDUs are sent as valid SecureMessaging APDUs. 3. This test case can only be done AFTER EAC2_ISO7816_M_3 has been performed.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be the trust point received in DO 87 as read returned by the PACE mechanism. 2. Send the appropriate link certificate 1 as specified in table 70. The PICC MUST update the trust point with this new certificate. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <certificate reference> • The Certification Authority Reference MUST be used as specified in the Link certificate used in step 2. 4. Send the appropriate link certificate 2 as specified in table 70. The ePassport MUST update the trust point with this new certificate. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 5. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as specified in the second Link certificate used in step 4. 6. Send the appropriate DV-Certificate as specified in table 70. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 7. Power off the chip, perform PACE again and verify the trust points returned by the PACE mechanism. Both new trust points must be present. The previous trust point from the LINK CERT 7 as specified in test case EAC2_ISO7816_M_3

	MUST be gone.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '90 00' within a valid Secure Messaging response. 7. true

Test Case ID	Version	Profile	Certificates	Password
EAC2_ISO7816_M_4a	EAC2_1.0	TA2_IS	Link Cert 1: LINK_CERT_8 Link Cert 2: LINK_CERT_9 DV Cert: DV_CERT_9	MRZ/CAN
EAC2_ISO7816_M_4b	Smart-eID	TA2_AT	Link Cert 1: LINK_CERT_8a Link Cert 2: LINK_CERT_9a DV Cert: DV_CERT_9a	PIN

Table 70: Test cases EAC2_ISO7816_M_4

3.8.5 Test case EAC2_ISO7816_M_5_Template

Before performing this test case, validate, that the trust point has successfully been updated in test cases EAC2_ISO7816_M_3 and EAC2_ISO7816_M_4.

Test - ID	EAC2_ISO7816_M_5_Template
Purpose	Test the transition CVCA \Rightarrow CVCA \Rightarrow IS/AT. This test changes the trust points.
Version	see table 71
Profile	see table 71
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using password specified in table 71. 2. All APDUs are sent as valid SecureMessaging APDUs. 3. This test case can only be done AFTER EAC2_ISO7816_M_4 has been performed.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. $'0C\ 22\ 81\ B6\ <Lc>\ 87\ <L_{87}>\ 01\ <Cryptogram>\ 8E\ 08\ <Checksum>\ 00'$ <ul style="list-style-type: none"> • $<Cryptogram>$ contains the following encrypted data objects $83\ <L_{83}>\ <Certification\ Authority\ Reference>$ • The Certification Authority Reference MUST be used as returned by the PACE mechanism (Primary trust point, i.e. DO87). 2. Send the appropriate link certificate as specified in table 71. $'0C\ 2A\ 00\ BE\ <Lc>\ 87\ <L_{87}>\ 01\ <Cryptogram>\ 8E\ 08\ <Checksum>\ <Le>'$

Test plan for eID-Cards with EAC 2.0

	<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> <p>3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certificate Holder Reference stored inside the new CVCA-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS/AT-Certificate as specified in table 71. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response. '90 00' within a valid Secure Messaging response. '90 00' within a valid Secure Messaging response. Checking error or '63 00' in a SM response

Test Case ID	Version	Profile	Certificates	Password
EAC2_ISO7816_M_5a	EAC2_1.0	TA2_IS	Link Cert: LINK_CERT_11b IS Cert: IS_CERT_11c	MRZ/CAN
EAC2_ISO7816_M_5b	Smart-eID	TA2_AT	Link Cert: LINK_CERT_11c AT Cert: AT_CERT_11a	PIN

Table 71: Test cases EAC2_ISO7816_M_5

3.8.6 Test case EAC2_ISO7816_M_6

Before performing this test case, validate, that the trust point has successfully been updated in test case EAC2_ISO7816_M_3.

Test - ID	EAC2_ISO7816_M_6
Purpose	Test the “Trust Point” update mechanism dependency to other applications, i. e. all applications share the same current date, but have different trust points. This test works with AT trust points.
Version	EAC2_1.0
Profile	eID, TA2_AT
Preconditions	<ol style="list-style-type: none"> Validate that EAC2_ISO7816_M_3 has been performed successfully The PACE mechanism MUST have been performed using PIN. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card.

	<pre>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism (Primary trust point, i.e. DO87). <p>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 17” chapter asDV_CERT_17a.</p> <pre>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. some OS dependent error within a valid Secure Messaging response.

3.8.7 Test case EAC2_ISO7816_M_7

Before performing this test case, validate, that the trust point has successfully been updated in test cases EAC2_ISO7816_M_3, EAC2_ISO7816_M_4 and EAC2_ISO7816_M_5.

Test - ID	EAC2 ISO7816 M 7
Purpose	Test the “Trust Point” update mechanism with two link certificates. This test changes the AT trust points.
Version	EAC2 1.0
Profile	(eID or SMARTeID), TA2_AT
Preconditions	<ol style="list-style-type: none"> 1. Validate that EAC2_ISO7816_M_3, EAC2_ISO7816_M_4 and EAC2_ISO7816_M_5 have been performed successfully 2. The PACE mechanism MUST have been performed using PIN. 3. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. <pre>'0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism (Primary trust point, i.e. DO87). 2. Send the appropriate link certificate as specified in the “Certificate Set 23” as LINK_CERT_23a. The PICC MUST update the trust point with this new certificate. <pre>'0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 3. Power down the field or remove the PICC from the reader, so that the chip

	<p>loses all temporary information. This is done to prove, that the new trust point has been stored in persistent memory. Power up the chip again and perform PACE again and verify that the new trust point is at the first position and the previous one has been moved to the second position</p> <p>4 . Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be the trust point received in DO 87 as returned by the PACE mechanism. <p>5 . Send the appropriate link certificate as specified in the "Certificate Set 23" as LINK_CERT_23b. The PICC MUST update the trust point with this new certificate. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> <p>6 . Power down the field or remove the PICC from the reader, so that the chip loses all temporary information. This is done to prove, that the new trust point has been stored in persistent memory. Power up the chip again and perform PACE again and verify that the new trust point is at the first position and the previous one has been moved to the second position</p> <p>7 . Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be the trust point received in DO 87 as returned by the PACE mechanism. <p>8 . Send the appropriate DV-Certificate as specified in the "Certificate Set 23" as DV_CERT_23. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • Since the trust point is still valid, the certificate MUST be verified successfully.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. true 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. true 7. '90 00' within a valid Secure Messaging response.

	8. '90 00' within a valid Secure Messaging response.
--	--

3.8.8 Test case EAC2_ISO7816_M_8

Before performing this test case, validate that the trust points have successfully been updated in test cases EAC2_ISO7816_M_3, EAC2_ISO7816_M_4, EAC2_ISO7816_M_5 and EAC2_ISO7816_M_7

Test - ID	EAC2_ISO7816_M_8
Purpose	Test the “Trust Point” update mechanism independence to other applications. The IS trust points MUST NOT be affected by AT trust point updates. This test works with IS trust points.
Version	EAC2 1.0
Profile	TA2_IS
Preconditions	<ol style="list-style-type: none"> 1. Validate that EAC2_ISO7816_M_3, EAC2_ISO7816_M_4, EAC2_ISO7816_M_5 and EAC2_ISO7816_M_7 have been performed successfully 2. The PACE mechanism MUST have been performed using PIN. 3. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be the trust point received in DO 87 as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 11” as DV_CERT_11d. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response.

3.8.9 Test case EAC2_ISO7816_M_9

Test - ID	EAC2_ISO7816_M_9
Purpose	Positive test to verify that a link certificate can deactivate a feature of the eID card. In this test case the right to read DG1 is used to verify that the eID card supports deactivation of features by link certificates.
Version	EAC2 1.2
Profile	(eID or SMARTeID), TA2_AT, AUTH_EXT
Preconditions	<ol style="list-style-type: none"> 1. It MUST be assured that the eID chip has already access right to read DG1 2. The PACE mechanism MUST have been performed using PIN. 3. The TA2 mechanism MUST have been performed with DV_CERT_20a and

Test plan for eID-Cards with EAC 2.0

	<p>AT_CERT_20w</p> <p>4. All APDUs are sent as valid SecureMessaging APDUs.</p>
Test scenario	<p>1. Send the given Read Binary (with SFI) command to the eID Card, to verify the read access to the selected data group has been granted. `0C B0 81 00 0D 97 01 01 8E 08 <Checksum> 00'</p> <p>2. The PACE mechanism MUST have been performed (PIN).</p> <p>3. The TA2 mechanism MUST have been performed with LINK_CERT_32b</p> <p>4. The TA2 mechanism MUST have been performed with DV_CERT_20a and AT_CERT_20w</p> <p>5. Send the given Read Binary (with SFI) command to the eID Card, to verify the read access to the selected data group has been granted. `0C B0 81 00 0D 97 01 01 8E 08 <Checksum> 00'</p>
Expected results	<p>1. '<first byte of data group content data> 90 00' within a valid Secure Messaging response</p> <p>2. True.</p> <p>3. True.</p> <p>4. True.</p> <p>5. Checking error within a valid Secure Messaging response.</p>

3.8.10 Test case EAC2_ISO7816_M_10

Test - ID	EAC2_ISO7816_M_10
Purpose	Positive test to verify that a link certificate can activate a feature of the eID card. In this test case the right to read DG1 is used to verify that the eID card supports activation of features by link certificates.
Version	EAC2 1.2
Profile	(eID or SMARTeID), TA2_AT, AUTH_EXT
Preconditions	<p>1. It MUST be assured that the eID chip has no right to read DG1</p> <p>2. The PACE mechanism MUST have been performed using PIN .</p> <p>3. The TA2 mechanism MUST have been performed with DV_CERT_20a and AT_CERT_20w</p> <p>4. All APDUs are sent as valid SecureMessaging APDUs.</p>
Test scenario	<p>1. Send the given Read Binary (with SFI) command to the eID Card, to verify the read access to the selected data group has been granted. `0C B0 81 00 0D 97 01 01 8E 08 <Checksum> 00'</p> <p>2. The PACE mechanism MUST have been performed (PIN).</p> <p>3. The TA2 mechanism MUST have been performed with LINK_CERT_32a</p> <p>4. The TA2 mechanism MUST have been performed with DV_CERT_20a and AT_CERT_20w</p> <p>5. Send the given Read Binary (with SFI) command to the eID Card, to verify the read access to the selected data group has been granted. `0C B0 81 00 0D 97 01 01 8E 08 <Checksum> 00'</p>
Expected results	<p>1. Checking error within a valid Secure Messaging response.</p> <p>2. True.</p>

	<p>3. True.</p> <p>4. True.</p> <p>5. ‘<first byte of data group content data> 90 00’ within a valid Secure Messaging response.</p>
--	---

3.8.11 Test case EAC2_ISO7816_M_11

Test - ID	EAC2 ISO7816 M_11
Purpose	Positive test to verify that rights are granted by the last link certificate and not a combination of all rights in the whole certificate chain. In this test case the right to read DG1 is used.
Version	EAC2 1.2
Profile	(eID or SMARTeID), TA2_AT, AUTH_EXT
Preconditions	<ol style="list-style-type: none"> 1. It MUST be assured that the eID chip has no access right to read DG1 2. The PACE mechanism MUST have been performed using PIN . 3. The TA2 mechanism MUST have been performed with DV_CERT_20a and AT_CERT_20w 4. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given Read Binary (with SFI) command to the eID Card, to verify the read access to the selected data group has been granted. ‘0C B0 81 00 0D 97 01 01 8E 08 <Checksum> 00’ 2. The PACE mechanism MUST have been performed (PIN). 3. The TA2 mechanism MUST have been performed with LINK_CERT_32a 4. The TA2 mechanism MUST have been performed with DV_CERT_20a and AT_CERT_20w 5. Send the given Read Binary (with SFI) command to the eID Card, to verify the read access to the selected data group has been granted. ‘0C B0 81 00 0D 97 01 01 8E 08 <Checksum> 00’ 6. The PACE mechanism MUST have been performed (PIN). 7. The TA2 mechanism MUST have been performed with LINK_CERT_32b 8. The TA2 mechanism MUST have been performed with DV_CERT_20a and AT_CERT_20w 9. Send the given Read Binary (with SFI) command to the eID Card, to verify the read access to the selected data group has been granted. ‘0C B0 81 00 0D 97 01 01 8E 08 <Checksum> 00’
Expected results	<ol style="list-style-type: none"> 1. Checking error within a valid Secure Messaging response. 2. True. 3. True. 4. True. 5. ‘<first byte of data group content data> 90 00’ within a valid Secure Messaging response 6. True. 7. True. 8. True.

- | | |
|--|---|
| | 9. Checking error within a valid Secure Messaging response. |
|--|---|

3.8.12 Test case EAC2_ISO7816_M_12

Test - ID	EAC2_ISO7816_M_12
Purpose	Positive test to verify that a link certificate can activate a feature of the eID card. In this test case the right to compare DG8 is used to verify that the eID card supports activation of eID Access features by link certificates.
Version	EAC2_1.2
Profile	(eID or SMARTeID), TA2_AT, CMP, AUTH_EXT
Preconditions	<ol style="list-style-type: none"> 1. It MUST be assured that the eID chip has no right to compare DG8 2. The PACE mechanism MUST have been performed using PIN . 3. The TA2 mechanism MUST have been performed with DV_CERT_30a and AT_CERT_30y 4. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given Compare APDU to the eID Card. '0C 33 00 00 <L_c> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted <id-DGContent-DG8> 2. The PACE mechanism MUST have been performed using PIN. 3. The TA2 mechanism MUST have been performed with LINK_CERT_32c 4. The TA2 mechanism MUST have been performed with DV_CERT_30a and AT_CERT_30y 1. Send the given Compare APDU to the eID Card. '0C 33 00 00 <L_c> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted <id-DGContent-DG8>
Expected results	<ol style="list-style-type: none"> 1. Checking Error within a valid Secure Messaging response. 2. True. 3. True. 4. True. 5. '90 00' within a valid Secure Messaging response.

3.8.13 Test case EAC2_ISO7816_M_13

Test - ID	EAC2_ISO7816_M_13
Purpose	Positive test to verify that a link certificate can deactivate a feature of the eID card. In this test case the right to compare DG8 is used to verify that the eID card supports deactivation of eID Access features by link certificates.
Version	EAC2_1.2
Profile	(eID or SMARTeID), TA2_AT, CMP, AUTH_EXT
Preconditions	<ol style="list-style-type: none"> 1. It MUST be assured that the eID chip has right to compare DG8 2. The PACE mechanism MUST have been performed using PIN . 3. The TA2 mechanism MUST have been performed with DV_CERT_30a and

	<p>AT_CERT_30y</p> <p>4. All APDUs are sent as valid SecureMessaging APDUs.</p>
Test scenario	<ol style="list-style-type: none"> Send the given Compare APDU to the eID Card. '0C 33 00 00 <L_c> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted <id-DGContent-DG8> The PACE mechanism MUST have been performed using PIN . The TA2 mechanism MUST have been performed with LINK_CERT_32d The TA2 mechanism MUST have been performed with DV_CERT_30a and AT_CERT_30y Send the given Compare APDU to the eID Card. '0C 33 00 00 <L_c> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted <id-DGContent-DG8>
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response. True. True. True. Checking Error within a valid Secure Messaging response.

3.8.14 Test case EAC2_ISO7816_M_14

Test - ID	EAC2 ISO7816 M 14
Purpose	Positive test to verify that eID Access rights are granted by the last link certificate and not a combination of all rights in the whole certificate chain. In this test case the right to compare DG8 is used.
Version	EAC2 1.2
Profile	(eID or SMARTeID), TA2_AT, CMP, AUTH_EXT
Preconditions	<ol style="list-style-type: none"> It MUST be assured that the eID chip has no access right to compare DG8 The PACE mechanism MUST have been performed using PIN . The TA2 mechanism MUST have been performed with DV_CERT_30a and AT_CERT_30y All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given Compare APDU to the eID Card. '0C 33 00 00 <L_c> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the encrypted <id-DGContent-DG8> The PACE mechanism MUST have been performed using PIN . The TA2 mechanism MUST have been performed with LINK_CERT_32c The TA2 mechanism MUST have been performed with DV_CERT_30a and AT_CERT_30y Send the given Compare APDU to the eID Card. '0C 33 00 00 <L_c> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00'

	<p><Cryptogram> contains the encrypted <id-DGContent-DG8></p> <ol style="list-style-type: none"> 2. The PACE mechanism MUST have been performed (PIN). 3. The TA2 mechanism MUST have been performed with LINK_CERT_32d 4. The TA2 mechanism MUST have been performed with DV_CERT_30a and AT_CERT_30z 5. Send the given Compare APDU to the eID Card. '0C 33 00 00 <Lc> 85 <L85> <Cryptogram> 8E 08 <Checksum> 00' 6. <Cryptogram> contains the encrypted <id-DGContent-DG8>
Expected results	<ol style="list-style-type: none"> 1. Checking error within a valid Secure Messaging response. 2. True. 3. True. 4. True. 5. '90 00' within a valid Secure Messaging response 6. True. 7. True. 8. True. 9. Checking error within a valid Secure Messaging response.

3.9 Unit test EAC2_ISO7816_N – Migration policies

This unit covers all tests about the migration policies. This mechanism is used for the import of new CVCA key with new TA algorithm in post issuance phase.

The purpose of this unit is to ensure the migration policy(ies) claimed by the manufacturer can be implemented. This unit has to be performed once for each possible migration scenario and trust point indicated by the passport provider. After the algorithm has been updated, the full test specification has to be repeated based on this new algorithm.

Certificates of Certificate Set 13 are depending on the test cases executed in test suite M. Depending on the supported profiles (e.g. AUTH_EXT or AUTH_EXT_CMP) the updated date in the chip is different. On this way it might be needed to use an interim certificate to update the dates in the chip as required for test suite N.

3.9.1 Test case EAC2_ISO7816_N_1

Test - ID	EAC2_ISO7816_N_1
Purpose	Test of the TA mechanism migration according to the manufacturer's implementation statement. Replacement of the IS trust point.
Version	EAC2_1.0
Profile	TA2_IS, MIG
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed. 2. All APDUs are sent as valid SecureMessaging APDUs. 3. This test case can only be performed AFTER EAC2_ISO7816_M_5, EAC2_ISO7816_M_8 or EAC2_ISO7816_M_14 have been successfully performed including the interim certificate mentioned in the introduction of this chapter.

Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be the Trust point received in DO 87 as returned by the PACE mechanism. 2. Send the appropriate link certificate with the updated mechanism as defined in “Certificate Set 13” as LINK_CERT_13a. The ePassport MUST update the trust point with this new certificate. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <certificate reference> • The Certification Authority Reference MUST be used as specified in the Link certificate used in step 2. • The chip MUST be able to use the updated cryptographic algorithms as introduced by the link certificate in step 2. 4. Send the appropriate DV certificate as specified in the “Certificate Set 13” as DV_CERT_13a. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 5. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as specified in the DV Certificate used in step 4. 6. Send the appropriate IS-Certificate as specified in the “Certificate Set 13” as IS_CERT_13a. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response.

	<ol style="list-style-type: none"> 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '90 00' within a valid Secure Messaging response.
--	--

3.9.2 Test case EAC2_ISO7816_N_2

Test - ID	EAC2_ISO7816_N_2
Purpose	Test of the TA mechanism migration according to the manufacturer's implementation statement. Replacement of the AT trust point.
Version	EAC2 1.0
Profile	(eID or SMARTeID), TA2_AT, MIG
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN . 2. All APDUs are sent as valid SecureMessaging APDUs. 3. This test case can only be performed AFTER EAC2_ISO7816_M_5, EAC2_ISO7816_M_8 or EAC2_ISO7816_M_14 have been successfully performed including the interim certificate mentioned in the introduction of this chapter.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be the Trust point received in DO 87 as returned by the PACE mechanism. 2. Send the appropriate link certificate with the updated mechanism as defined in "Certificate Set 13" as LINK_CERT_13b. The ePassport MUST update the trust point with this new certificate. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <certificate reference> • The Certification Authority Reference MUST be used as specified in the Link certificate used in step 2. • The chip MUST be able to use the updated cryptographic algorithms as introduced by the link certificate in step 2. 4. Send the appropriate DV certificate as specified in the "Certificate Set 13" as DV_CERT_13b. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'

	<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> <p>5. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certification Authority Reference MUST be used as specified in the DV Certificate used in step 4. <p>6. Send the appropriate AT-Certificate as specified in the "Certificate Set 13" as IS_CERT_13b. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature>
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response.

3.10 Unit EAC2_ISO7816_O Effective Access Conditions with PACE CHAT Restrictions

This Unit extends Unit EAC2_ISO7816_L Effective Access Conditions. Most of the tests are repeated here, but the access is restricted by the CHAT submitted within the PACE mechanism.

3.10.1 Test case EAC2_ISO7816_O_1

Test - ID	EAC2_ISO7816_O_1
Purpose	Test with a valid terminal authentication process with access permission for DG 3 if the DV certificate permits access to DG 3 and DG 4 while the IS certificate enables only the access to DG 3 but CHAT forbids access to DG3.
Version	EAC2 1.0
Profile	ePassport, TA2_IS, DG3
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed using CAN. The following CHAT MUST be used: '02' All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects

	<p>83 <L₈₃> <Certification Authority Reference></p> <ul style="list-style-type: none"> The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 3” chapter as DV_CERT_3. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This DV-Certificate grants access to data group 3 and 4. <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS-Certificate as specified in the “Certificate Set 3” chapter as IS_CERT_3a. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This IS-Certificate grants only access to data group 3. <p>5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference > The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_03. <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting ePassport application): `0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted ePassport application-ID.
--	---

	<p>10. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 3 has not been granted. `0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. true 9. '90 00' within a valid Secure Messaging response. 10. Checking error within a valid Secure Messaging response.

3.10.2 Test case EAC2_ISO7816_O_2

Test – ID	EAC2 ISO7816 O 2
Purpose	Test with a valid terminal authentication process with access permission for DG 4 if the DV certificate permits access to DG 3 and DG 4 while the IS certificate enables only the access to DG 4 but CHAT forbids access to DG4.
Version	EAC2 1.0
Profile	ePassport, TA2 IS, DG4
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using CAN. The following CHAT MUST be used: '01' 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 3” chapter as DV_CERT_3 `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to data group 3 and 4. 3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference>

Test plan for eID-Cards with EAC 2.0

	<ul style="list-style-type: none"> The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS-Certificate as specified in the “Certificate Set 3” chapter as IS_CERT_3b. ‘0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>’</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This IS-Certificate grants only access to data group 4. <p>5. Send the given MSE: Set AT APDU to the eID Card. ‘0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00’</p> <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. ‘0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00’</p> <p>7. Send the given external authenticate command to the eID Card. ‘0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>’</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_03. <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting ePassport application): ‘0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00’</p> <ul style="list-style-type: none"> <Cryptogram> contains the encrypted ePassport application-ID. <p>10. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 4 has NOT been granted. ‘0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00’</p>
Expected results	<ol style="list-style-type: none"> ‘90 00’ within a valid Secure Messaging response. ‘<Eight bytes of random data> 90 00’ within a valid Secure Messaging response. ‘90 00’ within a valid Secure Messaging response. true ‘90 00’ within a valid Secure Messaging response. Checking error within a valid Secure Messaging response.

3.10.3 Test case EAC2_ISO7816_O_3

Test - ID	EAC2 ISO7816 O 3
Purpose	Test with a valid terminal authentication process for DG 3 if the DV certificate grant access to data group 3 only and the IS certificate enable access to both data 3 and 4 but CHAT forbids access to DG3.
Version	EAC2 1.0
Profile	ePassport, TA2_IS, DG3
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using CAN. The following CHAT MUST be used: '02' 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 4” chapter as DV_CERT_4 '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to data group 3 only. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate IS-Certificate as specified in the “Certificate Set 4” chapter as IS_CERT_4. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This IS-Certificate grants access to data group 3 and 4. 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference >

Test plan for eID-Cards with EAC 2.0

	<ul style="list-style-type: none"> The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_04. <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting ePassport application): '0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the encrypted ePassport application-ID. <p>10. Send the given Read Binary (with SFI) command to the eID Card, to verify the access to the data group 3 has NOT been granted. '0C B0 83 00 0D 97 01 01 8E 08 <Checksum> 00'</p> </p></p>
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. '90 00' within a valid Secure Messaging response. true '90 00' within a valid Secure Messaging response. Checking error within a valid Secure Messaging response.

3.10.4 Test case EAC2_ISO7816_O_4

Test - ID	EAC2 ISO7816 O_4
Purpose	Test with a valid terminal authentication process for DG 4 if the DV certificate grant access to data group 4 only and the IS certificate enables access to both data 3 and 4, but CHAT forbids access to data group 4.
Version	EAC2 1.0
Profile	ePassport, TA2_IS, DG4
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed using CAN. The following CHAT MUST be used: '01' All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects $83 <L_{83}> <\text{Certification Authority Reference}>$

	<ul style="list-style-type: none"> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 5” chapter as DV_CERT_5 `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to data group 4 only. <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate IS-Certificate as specified in the “Certificate Set 5” chapter as IS_CERT_5. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This IS-Certificate grants access to data group 3 and 4. <p>5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> • The Certificate Holder Reference stored inside the IS-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature created with the private key of IS_KEY_05. <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting ePassport application): `0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ePassport application-ID. <p>10. Send the given Read Binary (with SFI) command to the eID Card, to verify the</p>
--	---

	access to the data group 4 has NOT been granted. '0C B0 84 00 0D 97 01 01 8E 08 <Checksum> 00'
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. true 9. '90 00' within a valid Secure Messaging response. 10. Checking error within a valid Secure Messaging response.

3.10.5 Test case EAC2_ISO7816_O_5 Template

Test - ID	EAC2_ISO7816_O_5 template
Purpose	Test with a valid terminal authentication process with read access permission for well defined DGs if the DV certificate permits read access to all DGs while the Terminal certificate restricts access to one DG. DV certificate is an official domestic certificate. CHAT forbids access to the specific DG.
Version	See Table 72
Profile	SMARTeID or eID, TA2_AT, required data group presence see Table 72
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN. See Table 72 for CHAT that has to be used 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 19” chapter as DV_CERT_19. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants read access to all data groups. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference>

	<ul style="list-style-type: none"> The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 19” chapter as defined in Table 72, column <i>Cert Reference</i> `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> This Terminal-Certificate grants access to data groups as defined in Table 72, column <i>Access Rules</i>. <p>5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting eID application): `0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the encrypted eID application-ID. <p>10. Send the given Read Binary (with SFI) command to the eID Card, to verify the read access to the selected data group has NOT been granted. `0C B0 (80 <SFI>) 00 0D 97 01 01 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <SFI> contains the SFI reference as defined in Table 72, column <i>SFI</i>. </p> </p></p></p></p>
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. '90 00' within a valid Secure Messaging response. True '90 00' within a valid Secure Messaging response. Checking error within a valid Secure Messaging response.

Test case EAC2_ISO7816_O_5a to Test case EAC2_ISO7816_O_5v

Test Case ID	Version	Access Rules	Cert Reference	SFI
EAC2_ISO7816_O_5a	EAC2_1.0	This terminal certificate grants only read access to data group 1	AT_CERT_19a	0x01
EAC2_ISO7816_O_5b	EAC2_1.0	This terminal certificate grants only read access to data group 2	AT_CERT_19b	0x02
EAC2_ISO7816_O_5c	EAC2_1.0	This terminal certificate grants only read access to data group 3	AT_CERT_19c	0x03
EAC2_ISO7816_O_5d	EAC2_1.0	This terminal certificate grants only read access to data group 4	AT_CERT_19d	0x04
EAC2_ISO7816_O_5e	EAC2_1.0	This terminal certificate grants only read access to data group 5	AT_CERT_19e	0x05
EAC2_ISO7816_O_5f	EAC2_1.0	This terminal certificate grants only read access to data group 6	AT_CERT_19f	0x06
EAC2_ISO7816_O_5g	EAC2_1.0	This terminal certificate grants only read access to data group 7	AT_CERT_19g	0x07
EAC2_ISO7816_O_5h	EAC2_1.0	This terminal certificate grants only read access to data group 8	AT_CERT_19h	0x08
EAC2_ISO7816_O_5i	EAC2_1.0	This terminal certificate grants only read access to data group 9	AT_CERT_19i	0x09
EAC2_ISO7816_O_5j	EAC2_1.0	This terminal certificate grants only read access to data group 10	AT_CERT_19j	0x0a
EAC2_ISO7816_O_5k	EAC2_1.0	This terminal certificate grants only read access to data group 11	AT_CERT_19k	0x0b
EAC2_ISO7816_O_5l	EAC2_1.0	This terminal certificate grants only read access to data group 12	AT_CERT_19l	0x0c
EAC2_ISO7816_O_5m	EAC2_1.0	This terminal certificate grants only read access to data group 13	AT_CERT_19m	0x0d
EAC2_ISO7816_O_5n	EAC2_1.0	This terminal certificate grants only read access to data group 14	AT_CERT_19n	0x0e
EAC2_ISO7816_O_5o	EAC2_1.0	This terminal certificate grants only read access to data group 15	AT_CERT_19o	0x0f
EAC2_ISO7816_O_5p	EAC2_1.0	This terminal certificate grants only read access to data group 16	AT_CERT_19p	0x10
EAC2_ISO7816_O_5q	EAC2_1.0	This terminal certificate grants only read access to data group 17	AT_CERT_19q	0x11
EAC2_ISO7816_O_5r	EAC2_1.0	This terminal certificate grants only read access to data group 18	AT_CERT_19r	0x12
EAC2_ISO7816_O_5s	EAC2_1.0	This terminal certificate grants only read access to data group 19	AT_CERT_19s	0x13
EAC2_ISO7816_O_5t	EAC2_1.0	This terminal certificate grants only read access to data group 20	AT_CERT_19t	0x14
EAC2_ISO7816_O_5u	EAC2_1.0	This terminal certificate grants only read access to data group 21	AT_CERT_19u	0x15
EAC2_ISO7816_O_5v	EAC2_1.1	This terminal certificate grants only read access to data group 22	AT_CERT_19w	0x16

Table 72: Test cases EAC2_ISO7816_O_5

3.10.6 Test case EAC2_ISO7816_O_6 Template

Test - ID	EAC2_ISO7816_O_6 template
Purpose	Test with a valid terminal authentication process with read access permission for well defined DGs if the DV certificate permits read access to all DGs while the Terminal certificate restricts access to one DG. DV certificate is a non-official certificate. CHAT forbids access to the specific DG.
Version	See Table 73
Profile	SMARTeID or eID, TA2 AT, required data group presence see Table 73
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN. See Table 73 for CHAT to be used 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 20” chapter as DV_CERT_20. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants read access to all data groups. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 20” chapter as defined in Table 73, column Cert Reference '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to data groups as defined in Table 73, column Access Rules 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'

	<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <ol style="list-style-type: none"> 6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature 8. The Chip Authentication mechanism MUST be performed. 9. Send the given Select Application APDU to the eID Card (selecting eID application): '0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the encrypted eID application-ID. 10. Send the given Read Binary (with SFI) command to the eID Card, to verify the read access to the selected data group has NOT been granted. '0C B0 (80 <SFI>) 00 0D 97 01 01 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <SFI> contains the SFI reference as defined in Table 73, column <i>SFI</i>.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. True 9. '90 00' within a valid Secure Messaging response. 10. Checking error within a valid Secure Messaging response.

Test case EAC2_ISO7816_O_6a to Test case EAC2_ISO7816_O_6v:

Test Case ID	Version	Access Rules	Cert Reference	SFI	CHAT
EAC2_ISO7816_O_6a	EAC2_1.0	This terminal certificate grants only read access to data group 1	AT_CERT_20a	0x01	'3E 1F FF FE F7'
EAC2_ISO7816_O_6b	EAC2_1.0	This terminal certificate grants only read access to data group 2	AT_CERT_20b	0x02	'3E 1F FF FD F7'
EAC2_ISO7816_O_6c	EAC2_1.0	This terminal certificate grants only read access to data group 3	AT_CERT_20c	0x03	'3E 1F FF FB F7'
EAC2_ISO7816_O_6d	EAC2_1.0	This terminal certificate grants only read access to data group 4	AT_CERT_20d	0x04	'3E 1F FF F7 F7'
EAC2_ISO7816_O_6e	EAC2_1.0	This terminal certificate grants only read access to data group 5	AT_CERT_20e	0x05	'3E 1F FF EF F7'
EAC2_ISO7816_O_6f	EAC2_1.0	This terminal certificate grants only read access to data group 6	AT_CERT_20f	0x06	'3E 1F FF DF F7'
EAC2_ISO7816_O_6g	EAC2_1.0	This terminal certificate grants only read access to data group 7	AT_CERT_20g	0x07	'3E 1F FF BF F7'
EAC2_ISO7816_O_6h	EAC2_1.0	This terminal certificate grants only read access to data group 8	AT_CERT_20h	0x08	'3E 1F FF 7F F7'
EAC2_ISO7816_O_6i	EAC2_1.0	This terminal certificate grants only read access to data group 9	AT_CERT_20i	0x09	'3E 1F FE FF F7'
EAC2_ISO7816_O_6j	EAC2_1.0	This terminal certificate grants only read access to data group 10	AT_CERT_20j	0x0a	'3E 1F FD FF F7'
EAC2_ISO7816_O_6k	EAC2_1.0	This terminal certificate grants only read access to data group 11	AT_CERT_20k	0x0b	'3E 1F FB FF F7'
EAC2_ISO7816_O_6l	EAC2_1.0	This terminal certificate grants only read access to data group 12	AT_CERT_20l	0x0c	'3E 1F F7 FF F7'
EAC2_ISO7816_O_6m	EAC2_1.0	This terminal certificate grants only read access to data group 13	AT_CERT_20m	0x0d	'3E 1F EF FF F7'
EAC2_ISO7816_O_6n	EAC2_1.0	This terminal certificate grants only read access to data group 14	AT_CERT_20n	0x0e	'3E 1F DF FF F7'
EAC2_ISO7816_O_6o	EAC2_1.0	This terminal certificate grants only read access to data group 15	AT_CERT_20o	0x0f	'3E 1F BF FF F7'
EAC2_ISO7816_O_6p	EAC2_1.0	This terminal certificate grants only read access to data group 16	AT_CERT_20p	0x10	'3E 1F 7F FF F7'
EAC2_ISO7816_O_6q	EAC2_1.0	This terminal certificate grants only read access to data group 17	AT_CERT_20q	0x11	'3E 1E FF FF F7'
EAC2_ISO7816_O_6r	EAC2_1.0	This terminal certificate grants only read access to data group 18	AT_CERT_20r	0x12	'3E 1D FF FF F7'
EAC2_ISO7816_O_6s	EAC2_1.0	This terminal certificate grants only read access to data group 19	AT_CERT_20s	0x13	'3E 1B FF FF F7'
EAC2_ISO7816_O_6t	EAC2_1.0	This terminal certificate grants only read access to data group 20	AT_CERT_20t	0x14	'3E 17 FF FF F7'
EAC2_ISO7816_O_6u	EAC2_1.0	This terminal certificate grants only read access to data group 21	AT_CERT_20u	0x15	'3E 0F FF FF F7'
EAC2_ISO7816_O_6v	EAC2_1.1	This terminal certificate grants only read access to data group 22	AT_CERT_20v	0x16	'3E 1F FF FF F7'

Table 73: Test cases EAC2_ISO7816_O_6

3.10.7 Test case EAC2_ISO7816_O_7 Template

Test - ID	EAC2_ISO7816_O_7_template
Purpose	Test with a valid terminal authentication process with write access permission for well defined DGs if the DV certificate permits write access to all writable DGs while the Terminal certificate restricts access to one DG. DV certificate is an official domestic certificate. CHAT forbids access to the specific DG
Version	See Table 74
Profile	SMARTeID or eID, TA2_AT, required data group presence see Table 74
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN. See Table 74 for CHAT to be used. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 21” chapter as DV_CERT_21. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants write access to all writable data groups. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 21” chapter as referenced in Table 74, column <i>Cert Reference</i> '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to data groups as defined in Table 74, column <i>Access Rules</i>. 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'

Test plan for eID-Cards with EAC 2.0

	<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference > • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <ol style="list-style-type: none"> 6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the encrypted terminal generated signature 8. The Chip Authentication mechanism MUST be performed. 9. Send the given Select Application APDU to the eID Card (selecting eID application): '0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the encrypted eID application-ID. 10. Send the given Update Binary (with SFI) command to the eID Card, to verify that write access to the selected data group has NOT been granted. '0C D6 (80 <SFI>) 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: 01 02 03 04 • <SFI> contains the SFI reference as defined in Table 74, column SFI.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. True 9. '90 00' within a valid Secure Messaging response. 10. Checking error within a valid Secure Messaging response.

Test case EAC2_ISO7816_O_7a to Test case EAC2_ISO7816_O_7f:

Test Case ID	Version	Access Rules	Cert Reference	SFI	CHAT
EAC2_ISO7816_O_7a	EAC2_1.0	This terminal certificate grants only write access to data group 17	AT_CERT_21a	0x11	'1F 1F FF FF F7'
EAC2_ISO7816_O_7b	EAC2_1.0	This terminal certificate grants only write access to data group 18	AT_CERT_21b	0x12	'2F 1F FF FF F7'
EAC2_ISO7816_O_7c	EAC2_1.0	This terminal certificate grants only write access to data group 19	AT_CERT_21c	0x13	'37 1F FF FF F7'
EAC2_ISO7816_O_7d	EAC2_1.0	This terminal certificate grants only write access to data group 20	AT_CERT_21d	0x14	'3B 1F FF FF F7'
EAC2_ISO7816_O_7e	EAC2_1.0	This terminal certificate grants only write access to data group 21	AT_CERT_21e	0x15	'3D 1F FF FF F7'
EAC2_ISO7816_O_7f	EAC2_1.1	This terminal certificate grants only write access to data group 22	AT_CERT_21f	0x16	'3D 2F FF FF F7'

Table 74: Test cases EAC2_ISO7816_O_7

3.10.8 Test case EAC2_ISO7816_O_8 Template

Test - ID	EAC2_ISO7816_O_8 template
Purpose	Test with a valid terminal authentication process with write access permission for well defined DGs if the DV certificate permits write access to all writable DGs while the Terminal certificate restricts access to one DG. DV certificate is a non-official certificate. CHAT forbids access to the specific DG.
Version	See Table 75
Profile	SMARTeID or eID, TA2 AT, required data group presence see Table 75
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN. See Table 75 for CHAT to be used. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 22” chapter as DV_CERT_22. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants write access to all writable data groups. 3. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 22” chapter as defined in Table 75, column Cert Reference. '0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants only write access to data groups as defined in Table 75, column Access Rules. 5. Send the given MSE: Set AT APDU to the eID Card. '0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'

	<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting eID application): '0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted eID application-ID. <p>10. Send the given Update Binary (with SFI) command to the eID Card, to verify that write access to the selected data group has NOT been granted. '0C D6 (80 <SFI>) 00 0D <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: 01 02 03 04 • <SFI> contains the SFI reference as defined in Table 75, column <i>SFI</i>.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. True 9. '90 00' within a valid Secure Messaging response. 10. Checking error within a valid Secure Messaging response.

Test plan for eID Cards with EAC 2.0

Test case EAC2_ISO7816_O_8a to Test case EAC2_ISO7816_O_8f:

Test Case ID	Version	Access Rules	Cert Reference	SFI	CHAT
EAC2_ISO7816_O_8a	EAC2_1.0	This terminal certificate grants only write access to data group 17	AT_CERT_22a	0x11	'1F 1F FF FF F7'
EAC2_ISO7816_O_8b	EAC2_1.0	This terminal certificate grants only write access to data group 18	AT_CERT_22b	0x12	'2F 1F FF FF F7'
EAC2_ISO7816_O_8c	EAC2_1.0	This terminal certificate grants only write access to data group 19	AT_CERT_22c	0x13	'37 1F FF FF F7'
EAC2_ISO7816_O_8d	EAC2_1.0	This terminal certificate grants only write access to data group 20	AT_CERT_22d	0x14	'3B 1F FF FF F7'
EAC2_ISO7816_O_8e	EAC2_1.0	This terminal certificate grants only write access to data group 21	AT_CERT_22e	0x15	'3D 1F FF FF F7'
EAC2_ISO7816_O_8f	EAC2_1.1	This terminal certificate grants only write access to data group 22	AT_CERT_22f	0x16	'3D 2F FF FF F7'

Table 75: Test cases EAC2_ISO7816_O_8

3.10.9 Test case EAC2_ISO7816_O_9

Test - ID	EAC2_ISO7816_O_9
Purpose	Test with a valid terminal authentication process with rights for special functions if the DV certificate permits all special functions while the terminal certificate restricts access to one special function. DV certificate is an official domestic certificate. Special function allowed by terminal certificate is Age Verification. CHAT forbids age verification.
Version	EAC2 1.0
Profile	SMARTeID or eID, TA2_AT
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 17” chapter as DV_CERT_17. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to all eID special functions. 3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 17” chapter as AT_CERT_17f. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to special function “Age Verification” 5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'

Test plan for eID-Cards with EAC 2.0

	<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference > 67 <L₆₇> <Auxiliary Data> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. • Auxiliary Data contains valid Date of Birth data. <p>6. Send the given Get Challenge APDU to the eID Card. '0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. '0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting eID application): '0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted eID application-ID. <p>10. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. True 9. '90 00' within a valid Secure Messaging response. 10. '69 82' within a valid Secure Messaging response.

3.10.10 Test case EAC2_ISO7816_O_10

Test - ID	EAC2 ISO7816 O_10
Purpose	Test with a valid terminal authentication process with rights for special functions if the DV certificate permits all special functions while the terminal certificate restricts access to one special function. DV certificate is an official domestic certificate. Special function allowed by terminal certificate is Municipality ID Verification. CHAT forbids Municipality ID Verification.
Version	EAC2 1.0
Profile	SMARTeID or eID, TA2_AT

Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. 2. Send the appropriate DV-Certificate as specified in the “Certificate Set 17” chapter as DV_CERT_17. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to all eID special functions. 3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. 4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 17” chapter as AT_CERT_17g. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to special function “Age Verification” 5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference > 67 <L₆₇> <Auxiliary Data> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. • Auxiliary Data contains valid Municipality ID data. 6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00' 7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08

Test plan for eID-Cards with EAC 2.0

	<p><Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Select Application APDU to the eID Card (selecting eID application):</p> <p>'0C A4 04 0C <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted eID application-ID. <p>10. Send the given Verify APDU to the eID Card.</p> <p>'8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: <id-MunicipalityID>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. True 9. '90 00' within a valid Secure Messaging response. 10. '69 82'. The error MUST be encoded in a valid Secure Messaging response.

3.10.11 Test case EAC2_ISO7816_O_11

Test - ID	EAC2_ISO7816_O_11
Version	deleted in version 1.00 RC

3.10.12 Test case EAC2_ISO7816_O_12

Test - ID	EAC2_ISO7816_O_12
Purpose	Test with a valid terminal authentication process with rights for special functions if the DV certificate permits all special functions while the terminal certificate restricts access to one special function. DV certificate is an official domestic certificate. Special function allowed by terminal certificate is "PIN Management". CHAT forbids "PIN Management"
Version	EAC2_1.0
Profile	eID, TA2_AT
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN. 2. All APDUs are sent as valid SecureMessaging APDUs.
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'

	<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. <p>2. Send the appropriate DV-Certificate as specified in the “Certificate Set 17” chapter as DV_CERT_17. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This DV-Certificate grants access to all eID special functions. <p>3. Send the given MSE: Set DST APDU to the eID Card. `0C 22 81 B6 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>4. Send the appropriate Terminal-Certificate as specified in the “Certificate Set 17” chapter as AT_CERT_17b. `0C 2A 00 BE <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> • This Terminal-Certificate grants access to special function “PIN Management” <p>5. Send the given MSE: Set AT APDU to the eID Card. `0C 22 81 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 80 <L₈₀> <Cryptographic Mechanism Reference> 83 <L₈₃> <Certificate Holder Reference> • The Certificate Holder Reference stored inside the Terminal-Certificate sent in step 4 has to be used. <p>6. Send the given Get Challenge APDU to the eID Card. `0C 84 00 00 0D 97 01 08 8E 08 <Checksum> 00'</p> <p>7. Send the given external authenticate command to the eID Card. `0C 82 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted terminal generated signature <p>8. The Chip Authentication mechanism MUST be performed.</p> <p>9. Send the given Deactivate PIN APDU to the eID Card: `0C 04 10 03 <Lc> 8E 08 <Checksum> 00'</p>
Expected results	<ol style="list-style-type: none"> 1. ’90 00’ within a valid Secure Messaging response. 2. ’90 00’ within a valid Secure Messaging response.

	<ol style="list-style-type: none"> 3. '90 00' within a valid Secure Messaging response. 4. '90 00' within a valid Secure Messaging response. 5. '90 00' within a valid Secure Messaging response. 6. '<Eight bytes of random data> 90 00' within a valid Secure Messaging response. 7. '90 00' within a valid Secure Messaging response. 8. True 9. '69 82'. The error MUST be encoded in a valid Secure Messaging response.
--	---

3.11 Unit test EAC2_ISO7816_P – PIN-Management

This unit covers all tests about PINs. PINs are used for the ePassport, eID and eSign application. [R8] defines 4 types of PINs used in different contexts.

- **CAN:** The Card Access Number (CAN) is a short password that is printed or displayed on the document.
- **PIN:** The Personal Identification Number (PIN) is a short secret password that SHALL be only known to the legitimate holder of the document.
- **PUK:** The PIN Unblock Key (PUK) is a long secret password that SHALL be only known to the legitimate holder of the document.
- **MRZ:** The MRZ-Password is a secret key that is derived from the machine readable zone and may be used for both PACE and BAC.

3.11.1 Test case EAC2_ISO7816_P_1

Test – ID	EAC2 ISO7816 P 1
Purpose	Positive test case to reduce initial PIN retry counter by 1
Version	EAC2 1.02
Profile	PACE
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked, deactivated or suspended 2. PIN retry counter MUST be set to initial value 3. Use INVALID PIN for key derivation process
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card using PIN mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>' <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>'

	<p>4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>'</p> <p>5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>'</p> <p>6. Power off the chip and reinitialize connection</p> <p>7. Send the given MSE: Set AT APDU to the eID Card using PIN mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>'<ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. </p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7C}> '84' <L₈₄> <ephemeral public key> '90 00' 5. '63 00' or '63 CX' where X indicates the number of remaining verification tries, i.e. initial value – 1 (see ICS). 6. TRUE 7. '63 CX' where X indicates the number of remaining verification tries, i.e. initial value – 1 (see ICS).

3.11.2 Test case EAC2_ISO7816_P_2

Test – ID	EAC2 ISO7816 P 2
Purpose	Positive test case to reset PIN retry counter to initial value
Version	EAC2 1.02
Profile	PACE
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked, deactivated or suspended 2. This test case MUST be performed immediately after Test case EAC2_ISO7816_P_1. 3. Use VALID PIN for key derivation process
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card using PIN mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>'<ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce:

Test plan for eID-Cards with EAC 2.0

	<p>'10 86 00 00 <Lc> 7C 00 <Le>'</p> <p>3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7c}> 81 <L₈₁> <mapping data> <Le>'</p> <p>4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7c}> 83 <L₈₃> <ephemeral public key> <Le>'</p> <p>5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7c}> 85 <L₈₅> <authentication token> <Le>'</p> <p>6. Power off the chip and reinitialize connection</p> <p>7. Send the given MSE: Set AT APDU to the eID Card using PIN mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>'<ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. </p>
Expected results	<ol style="list-style-type: none"> 1. '63 CX' where X indicated the number of remaining verification tries, i.e. initial value – 1 (see ICS). 2. 7C <L_{7c}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7c}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7c}> '84' <L₈₄> <ephemeral public key> '90 00' 5. 7C <L_{7c}> '86' <L₈₆> <authentication token> '90 00' 6. TRUE 7. '90 00'

3.11.3 Test case EAC2_ISO7816_P_3

Test – ID	EAC2_ISO7816_P_3
Purpose	Positive test case to suspend PIN
Version	EAC2_1.02
Profile	PACE, NOT SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked, deactivated or suspended 2. Use INVALID PIN for key derivation process
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card using PIN mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>'<ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted

	<p>nonce: '10 86 00 00 <Lc> 7C 00 <Le>'</p> <ol style="list-style-type: none"> 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>' 5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>' 6. Power off the chip and reinitialize connection 7. Go to step 1 and repeat all steps until step 1 returns '63 C1'
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7C}> '84' <L₈₄> <ephemeral public key> '90 00' 5. '63 00' or '63 CX' where X indicates the number of remaining verification tries. 6. TRUE 7. '63 CX'. Repeat until X=1. The PICC MUST reduce X by 1 on each run.

3.11.4 Test case EAC2_ISO7816_P_4

Test – ID	EAC2_ISO7816_P_4
Purpose	Negative test case where PIN Authentication attempt with suspended PIN
Version	EAC2_1.0
Profile	PACE, NOT SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked or deactivated 2. The PIN MUST have been suspended (e.g. using Test case EAC2_ISO7816_P_3)
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card using PIN mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>'<ul style="list-style-type: none"> o PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. o The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement:

Test plan for eID-Cards with EAC 2.0

	<p>'10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>'</p> <p>5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>' • id-PACE-ECDH-GM-AES-CBC-CMAC-128</p>
Expected results	<ol style="list-style-type: none"> 1. '63 C1' 2. '90 00' or '69 85' or '69 82'. In case of an error the following steps can be skipped. 3. '90 00' or '69 85' or '69 82' 4. '90 00' or '69 85' or '69 82' 5. '69 85' or '69 82'

3.11.5 Test case EAC2_ISO7816_P_5

Test – ID	EAC2 ISO7816 P 5
Purpose	Positive test case where CAN Authentication attempt with suspended PIN, resume with PIN
Version	EAC2 1.02
Profile	PACE, NOT SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked or deactivated 2. The PIN MUST have been suspended (e.g. using Test case EAC2 ISO7816 P 3)
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card with CAN: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 02 84 <L₈₄> <PACE domain>' <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>' 5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>' 6. Send the given MSE: Set AT APDU to the eID Card. '0C 22 C1 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'

	<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects: 7C <L_{7C}> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain> PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. <p>7. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '1C 86 00 00 <Lc> 7C <L_{7C}> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects: '7C 00' </p> <p>8. Send the given General Authenticate APDU to the eID Card. '1C 86 00 00 <Lc> 7C <L_{7C}> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects: '7C <L_{7C}> 81 <L₈₁> <mapping data>' </p> <p>9. Send the given General Authenticate APDU to the eID Card. '1C 86 00 00 <Lc> 7C <L_{7C}> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects: '7C <L_{7C}> 83 <L₈₃> <ephemeral public key>' </p> <p>10. Send the given General Authenticate APDU to the eID Card. '0C 86 00 00 <Lc> 7C <L_{7C}> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects: '7C <L_{7C}> 85 <L₈₁> <authentication token>' </p> <p>11. Power off the chip and reinitialize connection</p> <p>12. Send the given MSE: Set AT APDU to the eID Card using PIN mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>' <ul style="list-style-type: none"> PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. </p>
Expected results	<ol style="list-style-type: none"> '90 00' 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 7C <L_{7C}> '84' <L₈₄> <ephemeral public key> '90 00' 7C <L_{7C}> '86' <L₈₆> <authentication token> '90 00' '63 C1' within a valid SM response

	<ol style="list-style-type: none"> 7. $7C <L_{7C}>$ '80' $<L_{80}>$ <encrypted nonce> '90 00' within a valid SM response 8. $7C <L_{7C}>$ '82' $<L_{82}>$ <mapping data> '90 00' within a valid SM response 9. $7C <L_{7C}>$ '84' $<L_{84}>$ <ephemeral public key> '90 00' within a valid SM response 10. $7C <L_{7C}>$ '86' $<L_{86}>$ <authentication token> '90 00' within a valid SM response 11. TRUE 12. '90 00'
--	---

3.11.6 Test case EAC2_ISO7816_P_6

Test – ID	EAC2_ISO7816_P_6
Purpose	Positive test case to check volatile resumed status of PIN using PACE with CAN
Version	EAC2 1.02
Profile	PACE, NOT SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked or deactivated 2. The PIN MUST have been suspended (e.g. using Test case EAC2_ISO7816_P_3)
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card with CAN: $'00 22 C1 A4 <Lc> 80 <L_{80}> <\text{PACE OID}> 83 01 02 84 <L_{84}> <\text{PACE domain}>'$ <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: $'10 86 00 00 <Lc> 7C 00 <Le>'$ 3. Send the given General Authenticate APDU to the eID Card to map the nonce: $'10 86 00 00 <Lc> 7C <L_{7C}> 81 <L_{81}> <\text{mapping data}> <Le>'$ 4. Perform key agreement: $'10 86 00 00 <Lc> 7C <L_{7C}> 83 <L_{83}> <\text{ephemeral public key}> <Le>'$ 5. Perform mutual authentication: $'00 86 00 00 <Lc> 7C <L_{7C}> 85 <L_{85}> <\text{authentication token}> <Le>'$ 6. Power off the chip and reinitialize connection 7. Send the given MSE: Set AT APDU to the eID Card using PIN mechanism: $'00 22 C1 A4 <Lc> 80 <L_{80}> <\text{PACE OID}> 83 01 03 84 <L_{84}> <\text{PACE domain}>'$ <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain

	parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess.
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7C}> '84' <L₈₄> <ephemeral public key> '90 00' 5. 7C <L_{7C}> '86' <L₈₆> <authentication token> '90 00' 6. TRUE 7. '63 C1'

3.11.7 Test case EAC2_ISO7816_P_7

Test – ID	EAC2_ISO7816_P_7
Purpose	Positive test case to change PIN
Version	EAC2 1.02
Profile	PACE
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked, deactivated or suspended 2. Use <u>VALID PIN</u> for key derivation process
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card using PIN mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>'<ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>' 5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>' 6. Send the given Reset Retry Counter APDU to the eID Card. '0C 2C 02 03 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '<new PIN>' 7. Power off the chip and reinitialize connection 8. Perform PACE to verify new PIN, e.g. using Test case EAC2_ISO7816_H_2

Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7C}> '84' <L₈₄> <ephemeral public key> '90 00' 5. 7C <L_{7C}> '86' <L₈₆> <authentication token> '90 00' 6. '90 00' within a valid SM response 7. TRUE 8. TRUE
------------------	--

3.11.8 Test case EAC2_ISO7816_P_8

Test – ID	EAC2_ISO7816_P_8
Purpose	Positive test case to block PIN
Version	EAC2 1.02
Profile	PACE, NOT SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked or deactivated 2. The PIN MUST have been suspended (e.g. using Test case EAC2_ISO7816_P_3) 3. Use INVALID PIN for key derivation process
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card using CAN mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 02 84 <L₈₄> <PACE domain>' <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>' 5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>' 6. Send the given MSE: Set AT APDU to the eID Card. '0C 22 C1 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: 7C <L_{7C}> 80 <L₈₀> <PACE OID>

	<p style="text-align: center;">83 01 03 84 <L₈₄> <PACE domain></p> <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. <p>7. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '1C 86 00 00 <Lc> 7C <L_{7c}> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects: '7C 00'</p> <p>8. Send the given General Authenticate APDU to the eID Card. '1C 86 00 00 <Lc> 7C <L_{7c}> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects: '7C <L_{7c}> 81 <L₈₁> <mapping data>'</p> <p>9. Send the given General Authenticate APDU to the eID Card. '1C 86 00 00 <Lc> 7C <L_{7c}> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects: '7C <L_{7c}> 83 <L₈₃> <ephemeral public key>'</p> <p>10. Send the given General Authenticate APDU to the eID Card. '0C 86 00 00 <Lc> 7C <L_{7c}> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' • <Cryptogram> contains the following encrypted data objects: '7C <L_{7c}> 85 <L₈₁> <authentication token>'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7c}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7c}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7c}> '84' <L₈₄> <ephemeral public key> '90 00' 5. 7C <L_{7c}> '86' <L₈₆> <authentication token> '90 00' 6. '63 C1' within a valid SM response 7. 7C <L_{7c}> '80' <L₈₀> <encrypted nonce> '90 00' within a valid SM response 8. 7C <L_{7c}> '82' <L₈₂> <mapping data> '90 00' within a valid SM response 9. 7C <L_{7c}> '84' <L₈₄> <ephemeral public key> '90 00' within a valid SM response 10. '63 00' or '63 C0' within a valid SM response

3.11.9 Test case EAC2_ISO7816_P_8a

Test – ID	EAC2 ISO7816 P 8a
Purpose	Positive test case where PIN Authentication attempt with blocked PIN

Test plan for eID-Cards with EAC 2.0

Version	EAC2 1.0, moved Test case EAC2 ISO7816 H 21
Profile	PACE
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been deactivated 2. The PIN MUST have been blocked (e.g. using Test case EAC2 ISO7816 P 8)
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card with PIN: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>' <ul style="list-style-type: none"> • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess.
Expected results	<ol style="list-style-type: none"> 1. '63 C0'

3.11.10 Test case EAC2 ISO7816 P 9

Test – ID	EAC2 ISO7816 P 9
Purpose	Positive test to unblock PIN while old PIN is used
Version	EAC2 1.02
Profile	PACE, NOT SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST have been blocked (e.g. using Test case EAC2 ISO7816 P 8) 2. Use VALID PUK for key derivation process 3. Use OLD PIN after unblock mechanism
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card using PUK mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 04 84 <L₈₄> <PACE domain>' <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>' 5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>' 6. Send the given Reset Retry Counter APDU to the eID Card. '0C 2C 03 03 <Lc> 8E 08 <Checksum> 00' 7. Power off the chip and reinitialize connection 8. Send the given MSE: Set AT APDU to the eID Card using OLD PIN

	<p>mechanism:</p> <p>'00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>'</p> <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess.
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7C}> '84' <L₈₄> <ephemeral public key> '90 00' 5. 7C <L_{7C}> '86' <L₈₆> <authentication token> '90 00' 6. '90 00' within a valid SM response 7. TRUE 8. '90 00'

3.11.11 Test case EAC2_ISO7816_P_10

Test – ID	EAC2 ISO7816 P_10
Purpose	Positive test to unblock PIN while NEW PIN is used
Version	EAC2 1.02
Profile	PACE, CNG PIN PUK
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST have been blocked(e.g. using Test case EAC2_ISO7816_P_8) 2. Use VALID PUK for key derivation process
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card using PUK mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 04 84 <L₈₄> <PACE domain>'<ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>' 5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>'

Test plan for eID-Cards with EAC 2.0

	<ol style="list-style-type: none"> 6. Send the given Reset Retry Counter APDU to the eID Card. '0C 2C 02 03 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '<new PIN>' 7. Power off the chip and reinitialize connection 8. Perform PACE to verify new PIN, e.g. using Test case EAC2_ISO7816_H_2
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7C}> '84' <L₈₄> <ephemeral public key> '90 00' 5. 7C <L_{7C}> '86' <L₈₆> <authentication token> '90 00' 6. '90 00' within a valid SM response 7. TRUE 8. TRUE

3.11.12 Test case EAC2_ISO7816_P_11

Test – ID	EAC2 ISO7816 P_11
Purpose	Positive test case to change PIN with PUK Authentication
Version	EAC2 1.02
Profile	PACE, CNG PIN PUK
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked, deactivated or suspended 2. Use VALID PUK for key derivation process
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card using PUK mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 04 84 <L₈₄> <PACE domain>' <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>' 5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>' 6. Send the given Reset Retry Counter APDU to the eID Card.

	<pre>'0C 2C 02 03 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</pre> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '<new PIN>' <ol style="list-style-type: none"> 7. Power off the chip and reinitialize connection 8. Perform PACE to verify new PIN, e.g. using Test case EAC2 ISO7816 H 2
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7C}> '84' <L₈₄> <ephemeral public key> '90 00' 5. 7C <L_{7C}> '86' <L₈₆> <authentication token> '90 00' 6. '90 00' within a valid SM response 7. TRUE 8. TRUE

3.11.13 Test case EAC2_ISO7816_P_12

Test – ID	EAC2 ISO7816 P 12
Purpose	Negative test to change PIN with PUK Authentication
Version	EAC2 1.02
Profile	PACE, NOT SMARTeID, NOT CNG PIN PUK
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked, deactivated or suspended 2. Use VALID PUK for key derivation process
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card using PUK mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 04 84 <L₈₄> <PACE domain>' <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>' 5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>' 6. Send the given Reset Retry Counter APDU to the eID Card. '0C 2C 02 03 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08

	<p><Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '<new PIN>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7c}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7c}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7c}> '84' <L₈₄> <ephemeral public key> '90 00' 5. 7C <L_{7c}> '86' <L₈₆> <authentication token> '90 00' 6. '69 82'. The error MUST be encoded in a valid Secure Messaging response.

3.11.14 Test case EAC2_ISO7816_P_13

Test – ID	EAC2 ISO7816 P_13
Purpose	Negative test to unblock PIN while using NEW PIN
Version	EAC2_1.02
Profile	PACE, NOT SMARTeID, NOT CNG_PIN_PUK
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST have been blocked(e.g. using Test case EAC2_ISO7816_P_8) 2. Use VALID PUK for key derivation process
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card using PUK mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 04 84 <L₈₄> <PACE domain>' <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7c}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7c}> 83 <L₈₃> <ephemeral public key> <Le>' 5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7c}> 85 <L₈₅> <authentication token> <Le>' 6. Send the given Reset Retry Counter APDU to the eID Card. '0C 2C 02 03 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '<new PIN>' 7. Power off the chip and reinitialize connection 8. Send the given MSE: Set AT APDU to the eID Card using OLD PIN

	<p>mechanism:</p> <p>'00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>'</p> <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess.
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7C}> '84' <L₈₄> <ephemeral public key> '90 00' 5. 7C <L_{7C}> '86' <L₈₆> <authentication token> '90 00' 6. '69 82'. The error MUST be encoded in a valid Secure Messaging response. 7. TRUE 8. '63 C0'. PIN MUST still be blocked.

3.11.15 Test case EAC2_ISO7816_P_14

Test – ID	EAC2 ISO7816 P 14
Purpose	Positive test case to change PIN
Version	EAC2 1.02
Profile	PACE
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked, deactivated or suspended 2. Use VALID PIN for key derivation process
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card using PIN mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>'<ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>' 5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>'

Test plan for eID-Cards with EAC 2.0

	<ol style="list-style-type: none"> 6. Send the given Reset Retry Counter APDU to the eID Card. '0C 2C 02 03 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '<new PIN>' 7. Power off the chip and reinitialize connection 8. Perform PACE to verify new PIN, e.g. using Test case EAC2_ISO7816_H_2
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7C}> '84' <L₈₄> <ephemeral public key> '90 00' 5. 7C <L_{7C}> '86' <L₈₆> <authentication token> '90 00' 6. '90 00' within a valid SM response 7. TRUE 8. TRUE

3.11.16 Test case EAC2_ISO7816_P_15

Test – ID	EAC2_ISO7816_P_15
Purpose	Positive test case to change PIN via authenticated PIN management
Version	EAC2 1.0
Profile	PACE, TA2_AT, CA2_CNG_PIN_AR
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, PIN management must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17b) 3. The Chip Authentication MUST have been performed 4. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Reset Retry Counter APDU to the eID Card. '0C 2C 02 03 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '<new PIN>' 2. Power off the chip and reinitialize connection 3. Perform PACE to verify new PIN, e.g. using Test case EAC2_ISO7816_H_2
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. TRUE 3. TRUE

3.11.17 Test case EAC2_ISO7816_P_16

Test – ID	EAC2_ISO7816_P_16
Purpose	Negative test case to change PIN via authenticated PIN management

Version	EAC2 1.0
Profile	PACE, TA2_AT, CA2, NOT CNG_PIN_AR
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, PIN management must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17b) 3. The Chip Authentication MUST have been performed 4. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Reset Retry Counter APDU to the eID Card. '0C 2C 02 03 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '<new PIN>'
Expected results	<ol style="list-style-type: none"> 1. '69 82' within a valid SM response

3.11.18 Test case EAC2_ISO7816_P_17

Test – ID	EAC2_ISO7816_P_17
Purpose	Positive test case to change CAN
Version	EAC2 1.0
Profile	PACE, TA2_AT, CA2, CNG_CAN_AR
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, PIN management must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17b) 3. The Chip Authentication MUST have been performed 4. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Reset Retry Counter APDU to the eID Card. '0C 2C 02 02 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '<new CAN>' 2. Power off the chip and reinitialize connection 3. Perform PACE to verify new CAN, e.g. using Test case EAC2_ISO7816_H_1
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid SM response 2. TRUE 3. TRUE

3.11.19 Test case EAC2_ISO7816_P_18

Test – ID	EAC2_ISO7816_P_18
Purpose	Negative test case to change CAN
Version	EAC2 1.0
Profile	PACE, NOT SMARTeID, TA2_AT, CA2, NOT CNG_CAN_AR

Test plan for eID-Cards with EAC 2.0

Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, PIN management must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17b) 3. The Chip Authentication MUST have been performed 4. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Reset Retry Counter APDU to the eID Card. '0C 2C 02 02 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '<new CAN>'
Expected results	<ol style="list-style-type: none"> 1. '69 82' within a valid SM response

3.11.20 Test case EAC2_ISO7816_P_19

Test – ID	EAC2_ISO7816_P_19
Purpose	Positive test case to verify correct behavior when PIN is deactivated
Version	EAC2 1.0, moved Test case EAC2_ISO7816_H_28
Profile	PACE, NOT SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST have been deactivated
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card with PIN: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>'<ul style="list-style-type: none"> • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess.
Expected results	<ol style="list-style-type: none"> 1. '62 83'

3.11.21 Test case EAC2_ISO7816_P_20

Test – ID	EAC2_ISO7816_P_20
Purpose	Positive test case to try to change PIN, but NEW PIN is too short
Version	EAC2 1.02
Profile	PACE
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked, deactivated or suspended 2. Use VALID PIN for key derivation process
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card using PIN mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>'<ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess.

	<ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>' 5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>' 6. Send the given Reset Retry Counter APDU to the eID Card. '0C 2C 02 03 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '<new PIN>' • NEW PIN MUST be shorter than minimum PIN length stated in ICS 7. Power off the chip and reinitialize connection 8. Perform PACE to verify OLD PIN is still valid, e.g. using Test case EAC2_ISO7816_H_2
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7C}> '84' <L₈₄> <ephemeral public key> '90 00' 5. 7C <L_{7C}> '86' <L₈₆> <authentication token> '90 00' 6. '69 82' or other error within a valid SM response 7. TRUE 8. TRUE

3.11.22 Test case EAC2_ISO7816_P_21

Test – ID	EAC2_ISO7816_P_21
Purpose	Positive test case to verify the chain: reduce initial PIN retry counter, reset PIN and perform PACE
Version	Smart-eID
Profile	SMARTeID, NOT CAPA
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked, deactivated or suspended 2. PIN retry counter MUST be set to initial value 3. Use INVALID PIN for key derivation process
Test scenario	<ol style="list-style-type: none"> 1. Perform test case EAC2_ISO7816_P_1 2. Perform test case EAC2_ISO7816_P_2 3. Perform test case EAC2_ISO7816_H_2

Expected results	<ol style="list-style-type: none"> 1. See test case EAC2_ISO7816_P_1 2. See test case EAC2_ISO7816_P_2 3. See test case EAC2_ISO7816_H_4
------------------	---

3.11.23 Test case EAC2_ISO7816_P_22

Test – ID	EAC2_ISO7816_P_22
Purpose	Positive test case with blocked PIN
Version	Smart-eID
Profile	SMARTeID, NOT CAPA
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked, deactivated or suspended 2. Use INVALID PIN for key derivation process
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eID Card using PIN mechanism: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>' <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eID Card to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7c}> 81 <L₈₁> <mapping data> <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7c}> 83 <L₈₃> <ephemeral public key> <Le>' 5. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7c}> 85 <L₈₅> <authentication token> <Le>' 6. Power off the chip and reinitialize connection 7. Go to step 1 and repeat all steps until step 1 returns '63 C0' 8. Send the given MSE: Set AT APDU to the eID Card using PIN mechanism with correct PIN: '00 22 C1 A4 <Lc> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>' <ul style="list-style-type: none"> • PACE OID is a valid PACE OID (e.g. id-PACE-ECDH-GM-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. 9. Send the given General Authenticate APDU to the eID Card to get the encrypted

	<p>nonce: '10 86 00 00 <Lc> 7C 00 <Le>'</p> <p>10. Send the given General Authenticate APDU to the eID Card to map the nonce: '10 86 00 00 <Lc> 7C <L_{7C}> 81 <L₈₁> <mapping data> <Le>'</p> <p>11. Perform key agreement: '10 86 00 00 <Lc> 7C <L_{7C}> 83 <L₈₃> <ephemeral public key> <Le>'</p> <p>12. Perform mutual authentication: '00 86 00 00 <Lc> 7C <L_{7C}> 85 <L₈₅> <authentication token> <Le>'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' 2. 7C <L_{7C}> '80' <L₈₀> <encrypted nonce> '90 00' 3. 7C <L_{7C}> '82' <L₈₂> <mapping data> '90 00' 4. 7C <L_{7C}> '84' <L₈₄> <ephemeral public key> '90 00' 5. '63 00' or '63 CX' where X indicates the number of remaining verification tries. 6. TRUE 7. '63 CX'. Repeat until X=0. The Smart-eID MUST reduce X by 1 on each run. 8. '63 C0' 9. '90 00' or '69 83' or '69 82' or '63C0'. In case of an error or warning ('63C0') the following steps can be skipped. 10. '90 00' or '69 83' or '69 82' 11. '90 00' or '69 83' or '69 82' 12. '69 83' or '69 82'

3.12 Unit test EAC2_ISO7816_Q Auxiliary Data Verification

This unit covers all tests about eID special functions “auxiliary data verification”, i. e. age verification, document validity verification and Municipality ID verification.

3.12.1 Test case EAC2_ISO7816_Q_1

Test – ID	EAC2 ISO7816 Q 1
Purpose	Positive age verification test, verification successful, official domestic certificate
Version	EAC2 1.0
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17f) 3. Auxiliary data with valid Date of Birth data object MUST have been sent by authorized terminal during Terminal Authentication mechanism. The date of

Test plan for eID-Cards with EAC 2.0

	<p>birth MUST fit the required age.</p> <ol style="list-style-type: none"> 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response.

3.12.2 Test case EAC2_ISO7816_Q_2

Test – ID	EAC2_ISO7816_Q_2
Purpose	Positive age verification test, verification fails, official domestic certificate
Version	EAC2 1.0
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17f) 3. Auxiliary data with valid Date of Birth data object MUST have been sent by authorized terminal during Terminal Authentication mechanism. The date of birth MUST NOT fit the required age. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth>
Expected results	<ol style="list-style-type: none"> 1. '63 00'. The error MUST be encoded in a valid Secure Messaging response.

3.12.3 Test case EAC2_ISO7816_Q_3

Test – ID	EAC2_ISO7816_Q_3
Purpose	Age verification test with unauthorized terminal, official domestic certificate
Version	EAC2 1.0
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17a)

	<ol style="list-style-type: none"> 3. Auxiliary data with valid Date of Birth data object MUST have been sent by unauthorized terminal during Terminal Authentication mechanism. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth>
Expected results	<ol style="list-style-type: none"> 1. '69 82'. The error MUST be encoded in a valid Secure Messaging response.

3.12.4 Test case EAC2_ISO7816_Q_4

Test – ID	EAC2 ISO7816 Q 4
Purpose	Age verification test with authorized terminal but without auxiliary data transmission, official domestic certificate
Version	EAC2 1.0
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed without optional transmission of auxiliary data (DV_CERT_17, AT_CERT_17f) 3. The Chip Authentication MUST have been performed 4. The eID application MUST have been selected 5. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth>
Expected results	<ol style="list-style-type: none"> 1. '6A 88'. The error MUST be encoded in a valid Secure Messaging response.

3.12.5 Test case EAC2_ISO7816_Q_5

Test – ID	EAC2 ISO7816 Q 5
Purpose	Positive age verification test, verification successful, non-official certificate
Version	EAC2 1.0
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_18, AT_CERT_18f) 3. Auxiliary data with valid Date of Birth data object MUST have been sent by

Test plan for eID-Cards with EAC 2.0

	<p>authorized terminal during Terminal Authentication mechanism. Date of birth MUST fit the required age.</p> <ol style="list-style-type: none"> 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response

3.12.6 Test case EAC2_ISO7816_Q_6

Test – ID	EAC2_ISO7816_Q_6
Purpose	Positive document validity verification test, verification successful, official domestic certificate
Version	EAC2_1.0
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17g) 3. Auxiliary data with valid Document Validity data object MUST have been sent by authorized terminal during Terminal Authentication mechanism. Its date MUST fit document validity, i.e. <expiration date>-1 . 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-DateOfExpiry>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response.

3.12.7 Test case EAC2_ISO7816_Q_7

Test – ID	EAC2_ISO7816_Q_7
Purpose	Document validity verification test, verification fails, official domestic certificate
Version	EAC2_1.0
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17g)

	<ol style="list-style-type: none"> 3. Auxiliary data with valid Document Validity data object MUST have been sent by authorized terminal during Terminal Authentication mechanism. Its date MUST NOT fit document validity, i.e. <expiration date>+1. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-DateOfExpiry>
Expected results	<ol style="list-style-type: none"> 1. '63 00'. The error MUST be encoded in a valid Secure Messaging response.

3.12.8 Test case EAC2_ISO7816_Q_8

Test – ID	EAC2_ISO7816_Q_8
Purpose	Document Validity verification test with authorized terminal but without auxiliary data transmission, official domestic certificate
Version	EAC2 1.0
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN 2. The Terminal Authentication mechanism MUST have been performed without optional transmission of auxiliary data (DV_CERT_17, AT_CERT_17g) 3. The Chip Authentication MUST have been performed 4. The eID application MUST have been selected 5. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-DateOfExpiry>
Expected results	<ol style="list-style-type: none"> 1. '6A 88'. The error MUST be encoded in a valid Secure Messaging response.

3.12.9 Test case EAC2_ISO7816_Q_9

Test – ID	EAC2_ISO7816_Q_9
Purpose	Positive Document Validity verification test, verification successful, non-official certificate
Version	EAC2 1.0
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_18, AT_CERT_18g) 3. Auxiliary data with valid Document Validity data object MUST have been sent

Test plan for eID-Cards with EAC 2.0

	<p>by authorized terminal during Terminal Authentication mechanism. Document Validity MUST include the current date.</p> <ol style="list-style-type: none"> 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-DateOfExpiry>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response.

3.12.10 Test case EAC2_ISO7816_Q_10

Test – ID	EAC2_ISO7816_Q_10
Purpose	Positive Municipality ID verification test, verification successful, official domestic certificate
Version	EAC2_1.0
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, Municipality ID verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17g) 3. Auxiliary data with valid Municipality ID data object MUST have been sent by authorized terminal during Terminal Authentication mechanism. Municipality ID MUST fit the required ID. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-MunicipalityID>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response.

3.12.11 Test case EAC2_ISO7816_Q_11

Test – ID	EAC2_ISO7816_Q_11
Purpose	MunicipalityID verification test, verification fails, official domestic certificate
Version	EAC2_1.0
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, Municipality ID verification must be allowed by CHAT

	<ol style="list-style-type: none"> 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17g) 1. Auxiliary data with valid MunicipalityID data object MUST have been sent by authorized terminal during Terminal Authentication mechanism. MunicipalityID MUST NOT fit the required ID. 2. The Chip Authentication MUST have been performed 3. The eID application MUST have been selected 4. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: <id-MunicipalityID>
Expected results	<ol style="list-style-type: none"> 1. '63 00'. The error MUST be encoded in a valid Secure Messaging response.

3.12.12 Test case EAC2_ISO7816_Q_12

Test – ID	EAC2_ISO7816_Q_12
Purpose	MunicipalityID verification test with unauthorized terminal, official domestic certificate
Version	EAC2 1.0
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, Municipality ID verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17a) 3. Auxiliary data with valid MunicipalityID data object MUST have been sent by unauthorized terminal during Terminal Authentication mechanism. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: <id-MunicipalityID>
Expected results	<ol style="list-style-type: none"> 1. '69 82'. The error MUST be encoded in a valid Secure Messaging response.

3.12.13 Test case EAC2_ISO7816_Q_13

Test – ID	EAC2_ISO7816_Q_13
Purpose	MunicipalityID verification test with authorized terminal but without auxiliary data transmission, official domestic certificate
Version	EAC2 1.0
Profile	SMARTeID or eID, AUX

Test plan for eID-Cards with EAC 2.0

Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, Municipality ID verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed without optional transmission of auxiliary data (DV_CERT_17, AT_CERT_17g) 3. The Chip Authentication MUST have been performed 4. The eID application MUST have been selected 5. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-MunicipalityID>
Expected results	<ol style="list-style-type: none"> 1. '6A 88'. The error MUST be encoded in a valid Secure Messaging response.

3.12.14 Test case EAC2_ISO7816_Q_14

Test – ID	EAC2_ISO7816_Q_14
Purpose	Positive MunicipalityID verification test, verification successful, non-official certificate
Version	EAC2_1.0
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, Municipality ID verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_18, AT_CERT_18g) 3. Auxiliary data with valid MunicipalityID data object MUST have been sent by authorized terminal during Terminal Authentication mechanism. MunicipalityID MUST fit the required ID. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-MunicipalityID>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response

3.12.15 Test case EAC2_ISO7816_Q_15

Test – ID	EAC2_ISO7816_Q_15
Purpose	Positive Municipality ID verification test, verification successful, official domestic certificate, check leftmost part of Municipality ID
Version	EAC2_1.0
Profile	SMARTeID or eID, AUX

Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, Municipality ID verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17g) 3. Auxiliary data with valid Municipality ID data object MUST have been sent by authorized terminal during Terminal Authentication mechanism. MunicipalityID is truncated but the leftmost bytes MUST fit the required ID. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-MunicipalityID>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response.

3.12.16 Test case EAC2_ISO7816_Q_16

Test – ID	EAC2 ISO7816 Q 16
Purpose	Positive MunicipalityID verification test, verification successful, non-official certificate, check leftmost part of Municipality ID
Version	EAC2 1.0
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, Municipality ID verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_18, AT_CERT_18g) 3. Auxiliary data with valid MunicipalityID data object MUST have been sent by authorized terminal during Terminal Authentication mechanism. MunicipalityID is truncated but the leftmost bytes MUST fit the required ID. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-MunicipalityID>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response

3.12.17 Test case EAC2_ISO7816_Q_17

Test – ID	EAC2 ISO7816 Q 17
Purpose	Positive test with two Discretionary Data Templates in Authentication Data Object

Test plan for eID-Cards with EAC 2.0

	containing age verification data and document validity verification data, The verification must be successful with an official domestic certificate
Version	EAC2_1.1
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification and document verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17f) 3. Auxiliary data with valid Date of Birth data object and document validity data object MUST have been sent by an authorized terminal during Terminal Authentication mechanism. The date of birth and document validity MUST fit the required age and validity. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth> 2. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-DateOfExpiry>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response.

3.12.18 Test case EAC2_ISO7816_Q_18

Test – ID	EAC2_ISO7816_Q_18
Purpose	Positive test with three Discretionary Data Templates in Authentication Data Object containing age verification data, document validity verification data and MunicipalityID verification data. The verification must be successful with an official domestic certificate
Version	EAC2_1.1
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification and document verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17j) 3. Auxiliary data with valid Date of Birth data object, document validity data object and MunicipalityID data object MUST have been sent by an authorized terminal during Terminal Authentication mechanism. The date of birth, document validity and MunicipalityID MUST fit the required age, validity and MunicipalityID.

	<ol style="list-style-type: none"> 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth> 2. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects: <id-DateOfExpiry> 3. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: <id-MunicipalityID>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response.

3.12.19 Test case EAC2_ISO7816_Q_19

Test – ID	EAC2 ISO7816 Q 19
Purpose	Positive test with two Discretionary Data Templates of same type in Authentication Data Object containing two age verification data objects with same OID. The verification of last the data object must be successful with an official domestic certificate
Version	EAC2 1.1
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification and document verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17f) 3. Auxiliary data with two valid Date of Birth data objects MUST have been sent by an authorized terminal during Terminal Authentication mechanism. The first date of birth MUST NOT fit the required age, the second date of birth MUST fit the required age. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects:

Test plan for eID-Cards with EAC 2.0

	<id-DateOfBirth>
Expected results	1. '90 00' within a valid Secure Messaging response.

3.12.20 Test case EAC2_ISO7816_Q_20

Test – ID	EAC2_ISO7816_Q_20
Purpose	Negative test with two Discretionary Data Templates of the same type in the Authentication Data Object containing two age verification data objects with the same OID. The verification of last the data object must fail with an official domestic certificate
Version	EAC2_1.1
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification and document verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17f) 3. Auxiliary data with two valid Date of Birth data objects MUST have been sent by an authorized terminal during Terminal Authentication mechanism. The first date of birth MUST fit the required age, the second date of birth MUST NOT fit the required age. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth>
Expected results	1. Checking error or '63 00'in a valid Secure Messaging response.

3.12.21 Test case EAC2_ISO7816_Q_21

Test – ID	EAC2_ISO7816_Q_21
Purpose	Age verification test with authorized terminal but invalid auxiliary data object (wrong tag) and an official domestic certificate
Version	EAC2_1.1
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed with invalid (wrong tag 0x72 instead of 0x73) auxiliary data (DV_CERT_17, AT_CERT_17f). If the chip reacts at this step with a checking error, the following steps can be ignored and the chip has passed the test. 3. The Chip Authentication MUST have been performed 4. The eID application MUST have been selected 5. All APDUs are sent as valid Secure Messaging APDUs

Test scenario	<ol style="list-style-type: none"> Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth>
Expected results	<ol style="list-style-type: none"> '6A 88'. The error MUST be encoded in a valid Secure Messaging response.

3.12.22 Test case EAC2_ISO7816_Q_22

Test – ID	EAC2_ISO7816_Q_22
Purpose	Age verification test with authorized terminal but invalid auxiliary data object wrong OID tag) and an official domestic certificate
Version	EAC2_1.1
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed using PIN, age verification must be allowed by CHAT The Terminal Authentication mechanism MUST have been performed with invalid (wrong tag 0x07 instead of 0x06 for OID) auxiliary data (DV_CERT_17, AT_CERT_17f). If the chip reacts at this step with a checking error, the following steps can be ignored and the chip has passed the test. The Chip Authentication MUST have been performed The eID application MUST have been selected All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> Send the given Verify APDU to the eID Card. '8C 20 80 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth>
Expected results	<ol style="list-style-type: none"> '6A 88'. The error MUST be encoded in a valid Secure Messaging response.

3.13 Unit test EAC2_ISO7816_R Restricted Identification

This unit covers all tests about eID special function “restricted identification”.

Note: This test unit has to be performed for each key specified in ICS.

3.13.1 Test case EAC2_ISO7816_R_1

Test – ID	EAC2_ISO7816_R_1
Purpose	Positive test for Restricted Identification, official domestic certificate
Version	EAC2_1.0
Profile	SMARTeID or eID, RI
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed with PIN, restricted identification must be allowed by CHAT The Terminal Authentication MUST have been performed (DV_CERT_17,

Test plan for eID-Cards with EAC 2.0

	<p>AT_CERT_17c)</p> <ol style="list-style-type: none"> 3. The Chip Authentication MUST have been performed 4. The eID application MUST have been selected 5. All APDUs are sent as valid secure messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card: '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '80' <L₈₀> <id-RI-x> '84' <L₈₄> <RefKeyID> 2. Send the given General Authenticate APDU to the eID Card: '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the sector public key PK_{Sector} 7C <L_{7C}> 'A0' <L_{A0}> <PK_{Sector}>, Hash(PK_{Sector}) MUST fit the hash value encoded in AT_CERT_17c
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. 7C <L_{7C}> '81' <L₈₁> <I_{SectorPICC}> '90 00' in valid Secure Messaging response

3.13.2 Test case EAC2_ISO7816_R_2

Test – ID	EAC2_ISO7816_R_2
Version	deleted in version 1.00 RC

3.13.3 Test case EAC2_ISO7816_R_3

Test – ID	EAC2_ISO7816_R_3
Purpose	Test for Restricted Identification with unauthorized terminal, official domestic certificate
Version	EAC2 1.0
Profile	SMARTeID or eID, RI
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN, restricted identification must NOT be allowed by CHAT 2. The Terminal Authentication MUST have been performed (DV_CERT_17, AT_CERT_17c) 3. The Chip Authentication MUST have been performed 4. The eID application MUST have been selected 5. All APDUs are sent as valid secure messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card: '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '80' <L₈₀> <id-RI-x> '84' <L₈₄> <RefKeyID> 2. Send the given General Authenticate APDU to the eID Card: '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>'

	<ul style="list-style-type: none"> <Cryptogram> contains the sector public key PK_{Sector} $7C <L_{7C}> 'A0' <L_{A0}> <PK_{Sector}>$, Hash($PK_{Sector}$) MUST fit the hash value encoded in AT_CERT_17c
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response. expected result is CONDITIONAL: For private keys with “authorized only” attribute set: $'69 82'$. The error MUST be encoded in a valid Secure Messaging response. For private keys with “authorized only” attribute NOT set: $7C <L_{7C}> '81' <L_{81}> <I_{SectorPICC}> '90 00'$ in valid Secure Messaging response

3.13.4 Test case EAC2_ISO7816_R_4

Test – ID	EAC2_ISO7816_R_4
Version	deleted in version 1.00 RC

3.13.5 Test case EAC2_ISO7816_R_5

Test – ID	EAC2_ISO7816_R_5
Purpose	Test for Restricted Identification with unsupported algorithm, official domestic Certificate
Version	EAC2_1.0
Profile	SMARTeID or eID, RI
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed with PIN, restricted identification must be allowed by CHAT The Terminal Authentication MUST have been performed (DV_CERT_17, AT_CERT_17c) The Chip Authentication MUST have been performed The eID application MUST have been selected All APDUs are sent as valid secure messaging APDUs
Test scenario	<ol style="list-style-type: none"> Send the given MSE:Set AT APDU to the eID Card: $'0C 22 41 A4 <Lc> 87 <L_{87}> 01 <Cryptogram> 8E 08 <Checksum> 00'$ <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects: $'80' <L_{80}> <BadOID> '84' <L_{84}> <RefKeyID>$ (Use 0.4.0.127.0.7.2.2.2.5.1 as BadOID)
Expected results	<ol style="list-style-type: none"> Checking error in valid Secure Messaging response

3.13.6 Test case EAC2_ISO7816_R_6

Test – ID	EAC2_ISO7816_R_6
Purpose	Test for Restricted Identification with invalid sector public key, official domestic Certificate
Version	EAC2_1.0
Profile	SMARTeID or eID, RI

Test plan for eID-Cards with EAC 2.0

Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN, restricted identification must be allowed by CHAT 2. The Terminal Authentication MUST have been performed (DV_CERT_17, AT_CERT_17c) 3. The Chip Authentication MUST have been performed 4. The eID application MUST have been selected 5. All APDUs are sent as valid secure messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card: '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'<ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '80' <L₈₀> <id-RI-x> '84' <L₈₄> <RefKeyID> 2. Send the given General Authenticate APDU to the eID Card: '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>'<ul style="list-style-type: none"> • <Cryptogram> contains an invalid sector public key BAD_PK_{Sector} 7C <L_{7C}> 'A0' <L_{A0}> <BAD_PK_{Sector}> • <BAD_PK_{Sector}> is a sector public key which MUST differ from <PK_{Sector}>, i.e. hash(<BAD_PK_{Sector}>) MUST differ from the hash value encoded within terminal sector extension in AT CERT 17c
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. '63 00' or '6A 80'. The error MUST be encoded in a valid Secure Messaging response.

3.13.7 Test case EAC2_ISO7816_R_7

Test – ID	EAC2 ISO7816 R 7
Version	deleted in version 1.00 RC

3.13.8 Test case EAC2_ISO7816_R_8

Test – ID	EAC2 ISO7816 R 8
Purpose	Positive test for Restricted Identification, non-official Certificate
Version	EAC2_1.0
Profile	SMARTeID or eID, RI
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN, restricted identification must be allowed by CHAT 2. The Terminal Authentication MUST have been performed (DV_CERT_18, AT_CERT_18c) 3. The Chip Authentication MUST have been performed 4. The eID application MUST have been selected 5. All APDUs are sent as valid secure messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card: '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'

	<ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects: '80' <L₈₀> <id-RI-x> '84' <L₈₄> <RefKeyID> <p>2. Send the given General Authenticate APDU to the eID Card: '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> <Cryptogram> contains the sector public key PK_{Sector} 7C <L_{7C}> 'A0' <L_{A0}> <PK_{Sector}>, Hash(PK_{Sector}) MUST fit the hash value encoded in AT_CERT_18c
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response 7C <L_{7C}> '81' <L₈₁> <I_{SectorPICC}> '90 00' in valid Secure Messaging response

3.13.9 Test case EAC2_ISO7816_R_9

Test – ID	EAC2 ISO7816 R 9
Version	deleted in version 1.00 RC

3.13.10 Test case EAC2_ISO7816_R_10

Test – ID	EAC2 ISO7816 R 10
Purpose	Positive test for Restricted Identification, checking identical calculation of sector identifier
Version	EAC2 1.0
Profile	SMARTeID or eID, RI
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed with PIN, restricted identification must be allowed by CHAT The Terminal Authentication MUST have been performed (DV_CERT_24 AT_CERT_24) The Chip Authentication MUST have been performed The eID application MUST have been selected All APDUs are sent as valid secure messaging APDUs
Test scenario	<ol style="list-style-type: none"> Send the given MSE:Set AT APDU to the eID Card: '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects: '80' <L₈₀> <id-RI-x> '84' <L₈₄> <RefKeyID> Send the given General Authenticate APDU to the eID Card: '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the sector public key PK_{Sector} 7C <L_{7C}> 'A0' <L_{A0}> <PK_{Sector}>, Hash(PK_{Sector}) MUST fit the first hash value encoded in AT_CERT_24 Store returned <I_{SectorPICC}> Reset the chip after this step and restore the preconditions for this test case before the next step is performed. Send the given MSE:Set AT APDU to the eID Card:

Test plan for eID-Cards with EAC 2.0

	<p>'0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '80' <L₈₀> <id-RI-x> '84' <L₈₄> <RefKeyID> <p>6. Send the given General Authenticate APDU to the eID Card: '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>'</p> <ul style="list-style-type: none"> • <Cryptogram> contains the sector public key PK_{Sector} 7C <L_{7C}> 'A0' <L_{A0}> <PK_{Sector}>, Hash(PK_{Sector}) MUST fit the first hash value encoded in AT_CERT_24 <p>7. Stored <I_{SectorPICC}> MUST be identical to returned <I_{SectorPICC}></p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. 7C <L_{7C}> '81' <L₈₁> <I_{SectorPICC}> '90 00' within a valid Secure Messaging response 3. true 4. true 5. '90 00' within a valid Secure Messaging response 6. 7C <L_{7C}> '81' <L₈₁> <I_{SectorPICC}> '90 00' within a valid Secure Messaging response 7. true

3.13.11 Test case EAC2_ISO7816_R_11

Test – ID	EAC2 ISO7816 R 11
Version	deleted in version 1.00 RC

3.13.12 Test case EAC2_ISO7816_R_12

Test – ID	EAC2 ISO7816 R 12
Purpose	Positive test for Restricted Identification, checking different calculation of sector identifier with different sector public keys and identical secret key, “migration scenario”
Version	EAC2 1.0
Profile	SMARTeID or eID, RI
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed with PIN, restricted identification must be allowed by CHAT 2. The Terminal Authentication MUST have been performed (DV_CERT_24 AT_CERT_24) 3. The Chip Authentication MUST have been performed 4. The eID application MUST have been selected 5. All APDUs are sent as valid secure messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE:Set AT APDU to the eID Card: '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects:

	<p>'80' <L₈₀> <id-RI-x> '84' <L₈₄> <RefKeyID></p> <p>2. Send the given General Authenticate APDU to the eID Card: '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the sector public key PK_{Sector1} 7C <L_{7C}> 'A0' <L_{A0}> <PK_{Sector1}>, Hash(PK_{Sector1}) MUST fit the first hash value encoded in AT_CERT_24 <p>3. Store returned <I_{SectorPICC1}></p> <p>4. Send the given MSE:Set AT APDU to the eID Card: '0C 22 41 A4 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '80' <L₈₀> <id-RI-x> '84' <L₈₄> <RefKeyID> <p>5. Send the given General Authenticate APDU to the eID Card: '0C 86 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 97 <L₉₇> <Ne> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> • <Cryptogram> contains the sector public key PK_{Sector2} 7C <L_{7C}> 'A2' <L_{A2}> <PK_{Sector2}>, Hash(PK_{Sector2}) MUST fit the second hash value encoded in AT_CERT_24 <p>6. Stored <I_{SectorPICC1}> MUST be different to returned <I_{SectorPICC2}></p> </p></p></p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. 7C <L_{7C}> '81' <L₈₁> <I_{SectorPICC1}> '90 00' within a valid Secure Messaging response 3. true 4. '90 00' within a valid Secure Messaging response 5. 7C <L_{7C}> '83' <L₈₃> <I_{SectorPICC2}> '90 00' within a valid Secure Messaging response 6. true

3.14 Unit test EAC2_ISO7816_T_Envelope mechanism

This unit covers all tests about the envelope mechanism that can be used as an alternative to Extended Length. During this mechanism the commands ENVELOPE and GET RESPONSE are used to transmit commands or data in separate chunks. This mechanism can be used if the terminal or chip do not support Extended Length. PACE must be performed with CAN in case of TA2_IS and with PIN in case of TA2_AT.

3.14.1 Test case EAC2_ISO7816_T_1_Template

Test – ID	EAC2_ISO7816_T_1_Template
Purpose	Positive test of the ENVELOPE / GET RESPONSE mechanism where a chain of Envelope commands is sent to the ID card. This test case is based on ISO7816_J_1.
Version	EAC2_1.1
Profile	eID, (TA2_AT or TA2_IS), ENV, see table 76.
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed. 2. All envelope commands must be sent in plain, all enveloped APDUs are sent as

	<p>valid SecureMessaging APDUs.</p> <p>3. All enveloped response data MUST be SM protected.</p>
Test scenario	<p>1. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <L_c> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certification Authority Reference MUST be used as returned by the PACE mechanism. </p> <p>2. Send the following Envelope command without SM '10 C2 00 00 <L_c> <enveloped command>' with the following enveloped command (<enveloped command>) to the ID Card and a chunk size of 128 bytes: Send the appropriate DV-Certificate as specified in table 76. '0C 2A 00 BE <L_c> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <L_e>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> <p>Dependent on the length of the Verify Certificate command above, the Envelope command must be sent several times. The last Envelope command must use the CLA byte '00' to signal the last element of the chain.</p> <p>3. Send the following Get Response command to the ID card: '00 C0 00 00 00'</p> <p>4. Send the given MSE: Set DST APDU to the eID Card. '0C 22 81 B6 <L_c> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 83 <L₈₃> <Certification Authority Reference> • The Certificate Holder Reference stored inside the DV-Certificate sent in step 2 has to be used. <p>5. Send the following Envelope command without SM '10 C2 00 00 <L_c> <enveloped command>' with the following enveloped command (<enveloped command>) to the ID Card and a chunk size of 128 bytes similar to step 2: Send the appropriate IS/AT-Certificate as specified in table 76. '0C 2A 00 BE <L_c> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <L_e>' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects 7F 4E <L_{7F4E}> <certificate body> 5F 37 <L_{5F37}> <certificate signature> <p>Dependent on the length of the Verify Certificate command above, the Envelope command must be sent several times. The last Envelope command must use the CLA byte '00' to signal the last element of the chain.</p> <p>6. Send the following Get Response command to the eID Card: '00 C0 00 00 00'</p> </p></p></p>

Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. All Envelope commands must return '90 00' in plain, except the last Envelope command must return '61 xx' 3. Get Response command must return '90 00' in plain The enveloped Verify Certificate command must return '90 00' within a valid Secure Messaging response 4. '90 00' within a valid Secure Messaging response 5. All Envelope commands must return '90 00' in plain, except the last Envelope command must return '61 xx' 6. Get Response command must return '90 00' in plain The enveloped Verify Certificate command must return '90 00' within a valid Secure Messaging response
------------------	--

Test Case ID	Version	Profile	Certificates
EAC2_ISO7816_T_1a	EAC2_1.0	TA2_IS	Certificate Set 1: DV_CERT_1 and IS_CERT_1
EAC2_ISO7816_T_1b	Smart-eID	TA2_AT	Certificate Set 33: DV_CERT_33 and AT_CERT_33

Table 76: Test cases EAC2_ISO7816_T_1

3.14.2 Test case EAC2_ISO7816_T_2

Test – ID	EAC2_ISO7816_T_2
Purpose	Positive test of the ENVELOPE / GET RESPONSE mechanism where a chain of Get Response commands is sent to the ID card.
Version	EAC2_1.1
Profile	eID, ENV, (TA2_AT or TA2_IS), CA2, PACE, ePassport
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed 2. The Terminal Authentication MUST have been performed 3. The Chip Authentication MUST have been performed 4. The eMRTD application MUST have been selected 5. All enveloped APDUs are sent as valid secure messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the following Envelope command to the eID Card with an enveloped Read Binary command to read the first six bytes of EF.DG2: '00 C2 00 00 <Lc> 0C B0 82 00 0D 97 01 06 8E 08 <checksum> 00' 2. Send the following Get Response command to the eID Card: '00 C0 00 00 00'
Expected results	<ol style="list-style-type: none"> 1. '61 xx' in plain where xx is the number of remaining bytes 2. Get Response must return '90 00' Enveloped Read Binary command must return '90 00' within a valid Secure Messaging response At the end the returned data must include the first six bytes of DG2 and be valid.

3.14.3 Test case EAC2_ISO7816_T_3

Test – ID	EAC2_ISO7816_T_3
Purpose	Negative test of the ENVELOPE / GET RESPONSE mechanism to test that the chip reacts correct if a Get Response command is performed without a previous Envelope command.
Version	EAC2 1.1
Profile	eID, ENV
Preconditions	1. None, card recently activated
Test scenario	1. Send the given Get Response APDU to the eID Card: ‘00 C0 00 00 00’
Expected results	1. Checking error; the error code SHALL be returned as plain data without SM encoding and without any data

3.14.4 Test case EAC2_ISO7816_T_4

Test – ID	EAC2_ISO7816_T_4
Purpose	Negative test of the ENVELOPE / GET RESPONSE mechanism to test that the chip reacts correct if ENVELOPE / GET RESPONSE mechanism is performed in an SM channel.
Version	EAC2 1.1
Profile	eID, ENV
Preconditions	1. The PACE mechanism MUST have been performed 2. All APDUs are sent as valid secure messaging APDUs
Test scenario	1. Send the following Envelope command without SM ‘00 C2 00 00 <Lc> <enveloped command>’ with the following enveloped command (<enveloped command>) to the ID Card: ‘0C B0 (80 <sfi.EF.CardAccess>) 00 0D 97 01 01 8E 08 <checksum> 00’ 2. Send the given Get Response APDU to the eID Card: ‘0C C0 00 00 <Lc> 97 01 00 8E 08 <Checksum> 00’
Expected results	1. ‘61 xx’ in plain 2. Checking error in an SM encoded response APDU or Checking error in plain and a closed SM channel

3.14.5 Test case EAC2_ISO7816_T_5

Test – ID	EAC2_ISO7816_T_5
Purpose	Negative test of the ENVELOPE / GET RESPONSE mechanism to test that chip can return different status words – on the one hand a status word for the Envelope command and on the other hand a different status word for the enveloped command itself.
Version	EAC2 1.1
Profile	eID, ENV

Preconditions	1. None, card recently activated
Test scenario	1. Send the given Envelope APDU to the eID Card with an enveloped Read Binary (EF.CardSecurity) APDU: '00 C2 00 00 05 00 B0 9D 00 00' 2. Send the given Get Response APDU to the eID Card: '00 C0 00 00 00'
Expected results	1. '61 02' in plain 2. Get Response command: '90 00' in plain Enveloped status word: Checking error; the error code SHALL be returned as plain data without SM encoding and without any data

3.15 Unit test EAC2_ISO7816_U_Compare

This unit covers all tests about the command COMPARE that can be used to compare data groups in the eID application of the chip.

3.15.1 Test case EAC2_ISO7816_U_1_Template

Test – ID	EAC2 ISO7816 U 1
Purpose	Positive test of the Compare command. An official domestic certificate is used and the verification is successful.
Version	EAC2 1.1
Profile	SMARTeID or eID, CMP, AUTH_EXT, required data group presence see table 77
Preconditions	1. The PACE mechanism MUST have been performed using PIN, verification according to table 77 must be allowed by Authorization Extension bits in tag 65 in command MSE:Set AT 2. The Terminal Authentication mechanism MUST have been performed with the certificates defined in “Certificate Set 30“ chapter as DV_CERT_30 and AT_CERT as defined in table 77 3. Compare data with valid data object as defined in table 77 MUST have been sent by authorized terminal during Terminal Authentication mechanism. Sent data MUST match the content of tested data group 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	1. Send the given Compare APDU to the eID Card. '0C 33 00 00 <L _c > 85 <L ₈₅ > <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the encrypted ‘data object’ as defined in table 77
Expected results	1. '90 00' within a valid Secure Messaging response.

Test case EAC2_ISO7816_U_1a to test case EAC2_ISO7816_U_1v:

Testcase-ID	Version	Profile	Access Rules	Cert Reference	Data Object
EAC2_ISO7816_U_1a	EAC2_1.1	CMP.DG1	Compare DG1	AT_CERT_30a	id-DGContent-DG1
EAC2_ISO7816_U_1b	EAC2_1.1	CMP.DG2	Compare DG2	AT_CERT_30b	id-DGContent-DG2
EAC2_ISO7816_U_1c	EAC2_1.1	CMP.DG3	Compare DG3	AT_CERT_30c	id-DGContent-DG3
EAC2_ISO7816_U_1d	EAC2_1.1	CMP.DG4	Compare DG4	AT_CERT_30d	id-DGContent-DG4
EAC2_ISO7816_U_1e	EAC2_1.1	CMP.DG5	Compare DG5	AT_CERT_30e	id-DGContent-DG5
EAC2_ISO7816_U_1f	EAC2_1.1	CMP.DG6	Compare DG6	AT_CERT_30f	id-DGContent-DG6
EAC2_ISO7816_U_1g	EAC2_1.1	CMP.DG7	Compare DG7	AT_CERT_30g	id-DGContent-DG7
EAC2_ISO7816_U_1h	EAC2_1.1	CMP.DG8	Compare DG8	AT_CERT_30h	id-DGContent-DG8
EAC2_ISO7816_U_1i	EAC2_1.1	CMP.DG9	Compare DG9	AT_CERT_30i	id-DGContent-DG9
EAC2_ISO7816_U_1j	EAC2_1.1	CMP.DG10	Compare DG10	AT_CERT_30j	id-DGContent-DG10
EAC2_ISO7816_U_1k	EAC2_1.1	CMP.DG11	Compare DG11	AT_CERT_30k	id-DGContent-DG11
EAC2_ISO7816_U_1l	EAC2_1.1	CMP.DG12	Compare DG12	AT_CERT_30l	id-DGContent-DG12
EAC2_ISO7816_U_1m	EAC2_1.1	CMP.DG13	Compare DG13	AT_CERT_30m	id-DGContent-DG13
EAC2_ISO7816_U_1n	EAC2_1.1	CMP.DG14	Compare DG14	AT_CERT_30n	id-DGContent-DG14
EAC2_ISO7816_U_1o	EAC2_1.1	CMP.DG15	Compare DG15	AT_CERT_30o	id-DGContent-DG15
EAC2_ISO7816_U_1p	EAC2_1.1	CMP.DG16	Compare DG16	AT_CERT_30p	id-DGContent-DG16
EAC2_ISO7816_U_1q	EAC2_1.1	CMP.DG17	Compare DG17	AT_CERT_30q	id-DGContent-DG17
EAC2_ISO7816_U_1r	EAC2_1.1	CMP.DG18	Compare DG18	AT_CERT_30r	id-DGContent-DG18
EAC2_ISO7816_U_1s	EAC2_1.1	CMP.DG19	Compare DG19	AT_CERT_30s	id-DGContent-DG19
EAC2_ISO7816_U_1t	EAC2_1.1	CMP.DG20	Compare DG20	AT_CERT_30t	id-DGContent-DG20
EAC2_ISO7816_U_1u	EAC2_1.1	CMP.DG21	Compare DG21	AT_CERT_30u	id-DGContent-DG21
EAC2_ISO7816_U_1v	EAC2_1.1	CMP.DG22	Compare DG22	AT_CERT_30v	id-DGContent-DG22

Table 77: Test cases EAC2_ISO7816_U_1

3.15.2 Test case EAC2_ISO7816_U_2_Template

Test – ID	EAC2_ISO7816_U_2
Purpose	Negative test of the Compare command. An official domestic certificate is used and the verification fails.
Version	EAC2_1.1

Profile	SMARTeID or eID, CMP, AUTH_EXT, required data group presence see table 78
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, verification according to table 78 must be allowed by Authorization Extension bits in tag 65 in command MSE: Set AT 2. The Terminal Authentication mechanism MUST have been performed with the certificates defined in “Certificate Set 30“ chapter as DV_CERT_30 and AT_CERT according to table 78 3. During Terminal Authentication data to be compared MUST be sent with a valid data object as defined in table 78. The sent content MUST NOT match the content stored in corresponding data group 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Compare APDU to the eID Card. '0C 33 00 00 <L_c> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ‘data object’ as defined in table 78
Expected results	<ol style="list-style-type: none"> 1. ’63 40’. The error MUST be encoded in a valid Secure Messaging response.

Test case EAC2_ISO7816_U_2a to test case EAC2_ISO7816_U_2v:

Testcase-ID	Version	Profile	Access Rules	Cert Reference	Data Object
EAC2_ISO7816_U_2a	EAC2_1.1	CMP.DG1	Compare DG1	AT_CERT_30a	id-DGContent-DG1
EAC2_ISO7816_U_2b	EAC2_1.1	CMP.DG2	Compare DG2	AT_CERT_30b	id-DGContent-DG2
EAC2_ISO7816_U_2c	EAC2_1.1	CMP.DG3	Compare DG3	AT_CERT_30c	id-DGContent-DG3
EAC2_ISO7816_U_2d	EAC2_1.1	CMP.DG4	Compare DG4	AT_CERT_30d	id-DGContent-DG4
EAC2_ISO7816_U_2e	EAC2_1.1	CMP.DG5	Compare DG5	AT_CERT_30e	id-DGContent-DG5
EAC2_ISO7816_U_2f	EAC2_1.1	CMP.DG6	Compare DG6	AT_CERT_30f	id-DGContent-DG6
EAC2_ISO7816_U_2g	EAC2_1.1	CMP.DG7	Compare DG7	AT_CERT_30g	id-DGContent-DG7
EAC2_ISO7816_U_2h	EAC2_1.1	CMP.DG8	Compare DG8	AT_CERT_30h	id-DGContent-DG8
EAC2_ISO7816_U_2i	EAC2_1.1	CMP.DG9	Compare DG9	AT_CERT_30i	id-DGContent-DG9
EAC2_ISO7816_U_2j	EAC2_1.1	CMP.DG10	Compare DG10	AT_CERT_30j	id-DGContent-DG10
EAC2_ISO7816_U_2k	EAC2_1.1	CMP.DG11	Compare DG11	AT_CERT_30k	id-DGContent-DG11
EAC2_ISO7816_U_2l	EAC2_1.1	CMP.DG12	Compare DG12	AT_CERT_30l	id-DGContent-DG12
EAC2_ISO7816_U_2m	EAC2_1.1	CMP.DG13	Compare DG13	AT_CERT_30m	id-DGContent-DG13
EAC2_ISO7816_U_2n	EAC2_1.1	CMP.DG14	Compare DG14	AT_CERT_30n	id-DGContent-DG14
EAC2_ISO7816_U_2o	EAC2_1.1	CMP.DG15	Compare DG15	AT_CERT_30o	id-DGContent-DG15

Test plan for eID-Cards with EAC 2.0

Testcase-ID	Version	Profile	Access Rules	Cert Reference	Data Object
EAC2_ISO7816_U_2p	EAC2_1.1	CMP.DG16	Compare DG16	AT_CERT_30p	id-DGContent-DG16
EAC2_ISO7816_U_2q	EAC2_1.1	CMP.DG17	Compare DG17	AT_CERT_30q	id-DGContent-DG17
EAC2_ISO7816_U_2r	EAC2_1.1	CMP.DG18	Compare DG18	AT_CERT_30r	id-DGContent-DG18
EAC2_ISO7816_U_2s	EAC2_1.1	CMP.DG19	Compare DG19	AT_CERT_30s	id-DGContent-DG19
EAC2_ISO7816_U_2t	EAC2_1.1	CMP.DG20	Compare DG20	AT_CERT_30t	id-DGContent-DG20
EAC2_ISO7816_U_2u	EAC2_1.1	CMP.DG21	Compare DG21	AT_CERT_30u	id-DGContent-DG21
EAC2_ISO7816_U_2v	EAC2_1.1	CMP.DG22	Compare DG22	AT_CERT_30v	id-DGContent-DG22

Table 78: Test cases EAC2_ISO7816_U_2

3.15.3 Test case EAC2_ISO7816_U_3_Template

Test – ID	EAC2_ISO7816_U_3
Purpose	Negative test of Compare, verification fails because of unauthorized certificate, official domestic certificate
Version	EAC2_1.1
Profile	SMARTeID or eID, CMP, AUTH_EXT, required data group presence see table 79
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed using PIN, verification according to table 79 must be allowed by Authorization Extension bits in tag 65 in command MSE:Set AT The Terminal Authentication mechanism MUST have been performed with the certificates defined in “Certificate Set 30“ chapter as DV_CERT_30 and AT_CERT_30w as defined in table 79 Compare data with valid data object as defined in table 79 MUST have been sent by an authorized terminal during the Terminal Authentication mechanism. Sent data MUST match the content of tested data group The Chip Authentication MUST have been performed The eID application MUST have been selected All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> Send the given Compare APDU to the eID Card. '0C 33 00 00 <L_c> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the encrypted ‘data object’ as defined in table 79
Expected results	<ol style="list-style-type: none"> '69 82'. The error MUST be encoded in a valid Secure Messaging response.

Test case EAC2_ISO7816_U_3a to test case EAC2_ISO7816_U_3v:

Testcase-ID	Version	Profile	Access Rules	Cert Reference	Data Object
EAC2_ISO7816_U_3a	EAC2_1.1	CMP.DG1	Compare DG1	AT_CERT_30w	id-DGContent-DG1

Testcase-ID	Version	Profile	Access Rules	Cert Reference	Data Object
EAC2_ISO7816_U_3b	EAC2_1.1	CMP.DG2	Compare DG2	AT_CERT_30w	id-DGContent-DG2
EAC2_ISO7816_U_3c	EAC2_1.1	CMP.DG3	Compare DG3	AT_CERT_30w	id-DGContent-DG3
EAC2_ISO7816_U_3d	EAC2_1.1	CMP.DG4	Compare DG4	AT_CERT_30w	id-DGContent-DG4
EAC2_ISO7816_U_3e	EAC2_1.1	CMP.DG5	Compare DG5	AT_CERT_30w	id-DGContent-DG5
EAC2_ISO7816_U_3f	EAC2_1.1	CMP.DG6	Compare DG6	AT_CERT_30w	id-DGContent-DG6
EAC2_ISO7816_U_3g	EAC2_1.1	CMP.DG7	Compare DG7	AT_CERT_30w	id-DGContent-DG7
EAC2_ISO7816_U_3h	EAC2_1.1	CMP.DG8	Compare DG8	AT_CERT_30w	id-DGContent-DG8
EAC2_ISO7816_U_3i	EAC2_1.1	CMP.DG9	Compare DG9	AT_CERT_30w	id-DGContent-DG9
EAC2_ISO7816_U_3j	EAC2_1.1	CMP.DG10	Compare DG10	AT_CERT_30w	id-DGContent-DG10
EAC2_ISO7816_U_3k	EAC2_1.1	CMP.DG11	Compare DG11	AT_CERT_30w	id-DGContent-DG11
EAC2_ISO7816_U_3l	EAC2_1.1	CMP.DG12	Compare DG12	AT_CERT_30w	id-DGContent-DG12
EAC2_ISO7816_U_3m	EAC2_1.1	CMP.DG13	Compare DG13	AT_CERT_30w	id-DGContent-DG13
EAC2_ISO7816_U_3n	EAC2_1.1	CMP.DG14	Compare DG14	AT_CERT_30w	id-DGContent-DG14
EAC2_ISO7816_U_3o	EAC2_1.1	CMP.DG15	Compare DG15	AT_CERT_30w	id-DGContent-DG15
EAC2_ISO7816_U_3p	EAC2_1.1	CMP.DG16	Compare DG16	AT_CERT_30w	id-DGContent-DG16
EAC2_ISO7816_U_3q	EAC2_1.1	CMP.DG17	Compare DG17	AT_CERT_30w	id-DGContent-DG17
EAC2_ISO7816_U_3r	EAC2_1.1	CMP.DG18	Compare DG18	AT_CERT_30w	id-DGContent-DG18
EAC2_ISO7816_U_3s	EAC2_1.1	CMP.DG19	Compare DG19	AT_CERT_30w	id-DGContent-DG19
EAC2_ISO7816_U_3t	EAC2_1.1	CMP.DG20	Compare DG20	AT_CERT_30w	id-DGContent-DG20
EAC2_ISO7816_U_3u	EAC2_1.1	CMP.DG21	Compare DG21	AT_CERT_30w	id-DGContent-DG21
EAC2_ISO7816_U_3v	EAC2_1.1	CMP.DG22	Compare DG22	AT_CERT_30w	id-DGContent-DG22

Table 79: Test cases EAC2_ISO7816_U_3

3.15.4 Test case EAC2_ISO7816_U_4_Template

Test – ID	EAC2_ISO7816_U_4
Purpose	Negative test of the Compare command. The verification fails because no data for comparison has been transmitted. An official domestic certificate is used.
Version	EAC2_1.1
Profile	SMARTeID or eID, CMP, AUTH_EXT, required data group presence see table 80
Preconditions	1. The PACE mechanism MUST have been performed using PIN, verification as in

Test plan for eID-Cards with EAC 2.0

	<table border="1"> <tr> <td>table 80 must be allowed by Authorization Extension bits in tag 65 in command MSE:Set AT</td></tr> </table> <ol style="list-style-type: none"> 2. The Terminal Authentication mechanism MUST have been performed with the certificates defined in the “Certificate Set 30“ chapter as DV_CERT_30 and AT_CERT defined according to table 80 3. Compare data with valid data object as defined in table 80 MUST have been sent by authorized terminal during Terminal Authentication mechanism. Data to be compared MUST NOT be sent using a valid AAD including an DDT with empty discretionary data and valid OID 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs 	table 80 must be allowed by Authorization Extension bits in tag 65 in command MSE:Set AT
table 80 must be allowed by Authorization Extension bits in tag 65 in command MSE:Set AT		
Test scenario	<ol style="list-style-type: none"> 1. Send the given Compare APDU to the eID Card. '0C 33 00 00 <L_c> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ‘data object’ as defined in table 80 	
Expected results	<ol style="list-style-type: none"> 1. '6340'. The error MUST be encoded in a valid Secure Messaging response. 	

Test case EAC2_ISO7816_U_4a to test case EAC2_ISO7816_U_4v:

Testcase-ID	Version	Profile	Access Rules	Cert Reference	Data Object
EAC2_ISO7816_U_4a	EAC2_1.1	CMP.DG1	Compare DG1	AT_CERT_30a	id-DGContent-DG1
EAC2_ISO7816_U_4b	EAC2_1.1	CMP.DG2	Compare DG2	AT_CERT_30b	id-DGContent-DG2
EAC2_ISO7816_U_4c	EAC2_1.1	CMP.DG3	Compare DG3	AT_CERT_30c	id-DGContent-DG3
EAC2_ISO7816_U_4d	EAC2_1.1	CMP.DG4	Compare DG4	AT_CERT_30d	id-DGContent-DG4
EAC2_ISO7816_U_4e	EAC2_1.1	CMP.DG5	Compare DG5	AT_CERT_30e	id-DGContent-DG5
EAC2_ISO7816_U_4f	EAC2_1.1	CMP.DG6	Compare DG6	AT_CERT_30f	id-DGContent-DG6
EAC2_ISO7816_U_4g	EAC2_1.1	CMP.DG7	Compare DG7	AT_CERT_30g	id-DGContent-DG7
EAC2_ISO7816_U_4h	EAC2_1.1	CMP.DG8	Compare DG8	AT_CERT_30h	id-DGContent-DG8
EAC2_ISO7816_U_4i	EAC2_1.1	CMP.DG9	Compare DG9	AT_CERT_30i	id-DGContent-DG9
EAC2_ISO7816_U_4j	EAC2_1.1	CMP.DG10	Compare DG10	AT_CERT_30j	id-DGContent-DG10
EAC2_ISO7816_U_4k	EAC2_1.1	CMP.DG11	Compare DG11	AT_CERT_30k	id-DGContent-DG11
EAC2_ISO7816_U_4l	EAC2_1.1	CMP.DG12	Compare DG12	AT_CERT_30l	id-DGContent-DG12
EAC2_ISO7816_U_4m	EAC2_1.1	CMP.DG13	Compare DG13	AT_CERT_30m	id-DGContent-DG13
EAC2_ISO7816_U_4n	EAC2_1.1	CMP.DG14	Compare DG14	AT_CERT_30n	id-DGContent-DG14
EAC2_ISO7816_U_4o	EAC2_1.1	CMP.DG15	Compare DG15	AT_CERT_30o	id-DGContent-DG15
EAC2_ISO7816_U_4p	EAC2_1.1	CMP.DG16	Compare DG16	AT_CERT_30p	id-DGContent-DG16

Testcase-ID	Version	Profile	Access Rules	Cert Reference	Data Object
EAC2_ISO7816_U_4q	EAC2_1.1	CMP.DG17	Compare DG17	AT_CERT_30q	id-DGContent-DG17
EAC2_ISO7816_U_4r	EAC2_1.1	CMP.DG18	Compare DG18	AT_CERT_30r	id-DGContent-DG18
EAC2_ISO7816_U_4s	EAC2_1.1	CMP.DG19	Compare DG19	AT_CERT_30s	id-DGContent-DG19
EAC2_ISO7816_U_4t	EAC2_1.1	CMP.DG20	Compare DG20	AT_CERT_30t	id-DGContent-DG20
EAC2_ISO7816_U_4u	EAC2_1.1	CMP.DG21	Compare DG21	AT_CERT_30u	id-DGContent-DG21
EAC2_ISO7816_U_4v	EAC2_1.1	CMP.DG22	Compare DG22	AT_CERT_30v	id-DGContent-DG22

Table 80: Test cases EAC2_ISO7816_U_4**3.15.5 Test case EAC2_ISO7816_U_5_Template**

Test – ID	EAC2_ISO7816_U_5
Purpose	Positive test of Compare, verification successful, non-official certificate
Version	EAC2_1.1
Profile	SMARTeID or eID, CMP, AUTH_EXT, required data group presence see table 81
Preconditions	<ol style="list-style-type: none"> The PACE mechanism MUST have been performed using PIN, verification as in table 81 must be allowed by Authorization Extension bits in tag 65 in command MSE:Set AT The Terminal Authentication mechanism MUST have been performed with the certificates defined in “Certificate Set 31“ chapter as DV_CERT_31 and AT_CERT as defined in table 81 Compare data with valid data object as defined in table 81 MUST have been sent by authorized terminal during Terminal Authentication mechanism. The Chip Authentication MUST have been performed The eID application MUST have been selected All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> Send the given Compare APDU to the eID Card. '0C 33 00 00 <L_c> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> <Cryptogram> contains the encrypted ‘data object’ as defined in table 81
Expected results	<ol style="list-style-type: none"> '90 00' within a valid Secure Messaging response.

Test case EAC2_ISO7816_U_5a to test case EAC2_ISO7816_U_5v:

Testcase-ID	Version	Profile	Access Rules	Cert Reference	Data Object
EAC2_ISO7816_U_5a	EAC2_1.1	CMP.DG1	Compare DG1	AT_CERT_31a	id-DGContent-DG1
EAC2_ISO7816_U_5b	EAC2_1.1	CMP.DG2	Compare DG2	AT_CERT_31b	id-DGContent-DG2
EAC2_ISO7816_U_5c	EAC2_1.1	CMP.DG3	Compare DG3	AT_CERT_31c	id-DGContent-DG3

Testcase-ID	Version	Profile	Access Rules	Cert Reference	Data Object
EAC2_ISO7816_U_5d	EAC2_1.1	CMP.DG4	Compare DG4	AT_CERT_31d	id-DGContent-DG4
EAC2_ISO7816_U_5e	EAC2_1.1	CMP.DG5	Compare DG5	AT_CERT_31e	id-DGContent-DG5
EAC2_ISO7816_U_5f	EAC2_1.1	CMP.DG6	Compare DG6	AT_CERT_31f	id-DGContent-DG6
EAC2_ISO7816_U_5g	EAC2_1.1	CMP.DG7	Compare DG7	AT_CERT_31g	id-DGContent-DG7
EAC2_ISO7816_U_5h	EAC2_1.1	CMP.DG8	Compare DG8	AT_CERT_31h	id-DGContent-DG8
EAC2_ISO7816_U_5i	EAC2_1.1	CMP.DG9	Compare DG9	AT_CERT_31i	id-DGContent-DG9
EAC2_ISO7816_U_5j	EAC2_1.1	CMP.DG10	Compare DG10	AT_CERT_31j	id-DGContent-DG10
EAC2_ISO7816_U_5k	EAC2_1.1	CMP.DG11	Compare DG11	AT_CERT_31k	id-DGContent-DG11
EAC2_ISO7816_U_5l	EAC2_1.1	CMP.DG12	Compare DG12	AT_CERT_31l	id-DGContent-DG12
EAC2_ISO7816_U_5m	EAC2_1.1	CMP.DG13	Compare DG13	AT_CERT_31m	id-DGContent-DG13
EAC2_ISO7816_U_5n	EAC2_1.1	CMP.DG14	Compare DG14	AT_CERT_31n	id-DGContent-DG14
EAC2_ISO7816_U_5o	EAC2_1.1	CMP.DG15	Compare DG15	AT_CERT_31o	id-DGContent-DG15
EAC2_ISO7816_U_5p	EAC2_1.1	CMP.DG16	Compare DG16	AT_CERT_31p	id-DGContent-DG16
EAC2_ISO7816_U_5q	EAC2_1.1	CMP.DG17	Compare DG17	AT_CERT_31q	id-DGContent-DG17
EAC2_ISO7816_U_5r	EAC2_1.1	CMP.DG18	Compare DG18	AT_CERT_31r	id-DGContent-DG18
EAC2_ISO7816_U_5s	EAC2_1.1	CMP.DG19	Compare DG19	AT_CERT_31s	id-DGContent-DG19
EAC2_ISO7816_U_5t	EAC2_1.1	CMP.DG20	Compare DG20	AT_CERT_31t	id-DGContent-DG20
EAC2_ISO7816_U_5u	EAC2_1.1	CMP.DG21	Compare DG21	AT_CERT_31u	id-DGContent-DG21
EAC2_ISO7816_U_5v	EAC2_1.1	CMP.DG22	Compare DG22	AT_CERT_31v	id-DGContent-DG22

Table 81: Test cases EAC2_ISO7816_U_5

3.15.6 Test case EAC2_ISO7816_U_6 Template

Test – ID	EAC2_ISO7816_U_6
Purpose	Negative test of Compare, verification fail because of missing tag 65 for Authentication Extension in MSE:Set AT during PACE
Version	EAC2_1.1
Profile	SMARTeID or eID, CMP, AUTH_EXT, required data group presence see table 82
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, but without tag 65 in command MSE:Set AT 2. The Terminal Authentication mechanism MUST have been performed with the certificates defined in “Certificate Set 30“ chapter as DV_CERT_30 and

	<p>AT_CERT as defined in table 82</p> <ol style="list-style-type: none"> 3. Compare data with valid data object as defined in table 82 MUST have been sent by authorized terminal during Terminal Authentication mechanism. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Compare APDU to the eID Card. '0C 33 00 00 <L_c> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted 'data object' as defined in table 82
Expected results	<ol style="list-style-type: none"> 1. Checking error in valid Secure Messaging response.

Test case EAC2_ISO7816_U_6a to test case EAC2_ISO7816_U_6v:

Testcase-ID	Version	Profile	Access Rules	Cert Reference	Data Object
EAC2_ISO7816_U_6a	EAC2_1.1	CMP.DG1	Compare DG1	AT_CERT_30a	id-DGContent-DG1
EAC2_ISO7816_U_6b	EAC2_1.1	CMP.DG2	Compare DG2	AT_CERT_30b	id-DGContent-DG2
EAC2_ISO7816_U_6c	EAC2_1.1	CMP.DG3	Compare DG3	AT_CERT_30c	id-DGContent-DG3
EAC2_ISO7816_U_6d	EAC2_1.1	CMP.DG4	Compare DG4	AT_CERT_30d	id-DGContent-DG4
EAC2_ISO7816_U_6e	EAC2_1.1	CMP.DG5	Compare DG5	AT_CERT_30e	id-DGContent-DG5
EAC2_ISO7816_U_6f	EAC2_1.1	CMP.DG6	Compare DG6	AT_CERT_30f	id-DGContent-DG6
EAC2_ISO7816_U_6g	EAC2_1.1	CMP.DG7	Compare DG7	AT_CERT_30g	id-DGContent-DG7
EAC2_ISO7816_U_6h	EAC2_1.1	CMP.DG8	Compare DG8	AT_CERT_30h	id-DGContent-DG8
EAC2_ISO7816_U_6i	EAC2_1.1	CMP.DG9	Compare DG9	AT_CERT_30i	id-DGContent-DG9
EAC2_ISO7816_U_6j	EAC2_1.1	CMP.DG10	Compare DG10	AT_CERT_30j	id-DGContent-DG10
EAC2_ISO7816_U_6k	EAC2_1.1	CMP.DG11	Compare DG11	AT_CERT_30k	id-DGContent-DG11
EAC2_ISO7816_U_6l	EAC2_1.1	CMP.DG12	Compare DG12	AT_CERT_30l	id-DGContent-DG12
EAC2_ISO7816_U_6m	EAC2_1.1	CMP.DG13	Compare DG13	AT_CERT_30m	id-DGContent-DG13
EAC2_ISO7816_U_6n	EAC2_1.1	CMP.DG14	Compare DG14	AT_CERT_30n	id-DGContent-DG14
EAC2_ISO7816_U_6o	EAC2_1.1	CMP.DG15	Compare DG15	AT_CERT_30o	id-DGContent-DG15
EAC2_ISO7816_U_6p	EAC2_1.1	CMP.DG16	Compare DG16	AT_CERT_30p	id-DGContent-DG16
EAC2_ISO7816_U_6q	EAC2_1.1	CMP.DG17	Compare DG17	AT_CERT_30q	id-DGContent-DG17
EAC2_ISO7816_U_6r	EAC2_1.1	CMP.DG18	Compare DG18	AT_CERT_30r	id-DGContent-DG18
EAC2_ISO7816_U_6s	EAC2_1.1	CMP.DG19	Compare DG19	AT_CERT_30s	id-DGContent-DG19

Testcase-ID	Version	Profile	Access Rules	Cert Reference	Data Object
EAC2_ISO7816_U_6t	EAC2_1.1	CMP.DG20	Compare DG20	AT_CERT_30t	id-DGContent-DG20
EAC2_ISO7816_U_6u	EAC2_1.1	CMP.DG21	Compare DG21	AT_CERT_30u	id-DGContent-DG21
EAC2_ISO7816_U_6v	EAC2_1.1	CMP.DG22	Compare DG22	AT_CERT_30v	id-DGContent-DG22

Table 82: Test cases EAC2_ISO7816_U_6**3.15.7 Test case EAC2_ISO7816_U_7_Template**

Test – ID	EAC2_ISO7816_U_7
Purpose	Negative test of the Compare mechanism. The verification fails because of a mismatch between the access rights used during PACE encoded in the Authorization Extensions bits sent by the MSE: Set AT command and the access rights of the certificate used during TA.
Version	EAC2_1.1
Profile	SMARTeID or eID, CMP, AUTH_EXT, required data group presence see table 83
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, verification according to table 83 must not be allowed by Authorization Extension bits in tag 65. Use Authorization Extensions without any rights. 2. The Terminal Authentication mechanism MUST have been performed with the certificates defined in “Certificate Set 30“ chapter as DV_CERT_30 and AT_CERT as defined in table 83 3. Compare data with valid data object as defined in table 83 MUST have been sent by authorized terminal during Terminal Authentication mechanism. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Compare APDU to the eID Card. '0C 33 00 00 <L_c> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted ‘data object’ as defined in table 83
Expected results	<ol style="list-style-type: none"> 1. Checking error in valid Secure Messaging response.

Test case EAC2_ISO7816_U_7a to test case EAC2_ISO7816_U_7v:

Testcase-ID	Version	Profile	Access Rules	Cert Reference	Data Object
EAC2_ISO7816_U_7a	EAC2_1.1	CMP.DG1	Compare DG1	AT_CERT_30a	id-DGContent-DG1
EAC2_ISO7816_U_7b	EAC2_1.1	CMP.DG2	Compare DG2	AT_CERT_30b	id-DGContent-DG2
EAC2_ISO7816_U_7c	EAC2_1.1	CMP.DG3	Compare DG3	AT_CERT_30c	id-DGContent-DG3
EAC2_ISO7816_U_7d	EAC2_1.1	CMP.DG4	Compare DG4	AT_CERT_30d	id-DGContent-DG4

Testcase-ID	Version	Profile	Access Rules	Cert Reference	Data Object
EAC2_ISO7816_U_7e	EAC2_1.1	CMP.DG5	Compare DG5	AT_CERT_30e	id-DGContent-DG5
EAC2_ISO7816_U_7f	EAC2_1.1	CMP.DG6	Compare DG6	AT_CERT_30f	id-DGContent-DG6
EAC2_ISO7816_U_7g	EAC2_1.1	CMP.DG7	Compare DG7	AT_CERT_30g	id-DGContent-DG7
EAC2_ISO7816_U_7h	EAC2_1.1	CMP.DG8	Compare DG8	AT_CERT_30h	id-DGContent-DG8
EAC2_ISO7816_U_7i	EAC2_1.1	CMP.DG9	Compare DG9	AT_CERT_30i	id-DGContent-DG9
EAC2_ISO7816_U_7j	EAC2_1.1	CMP.DG10	Compare DG10	AT_CERT_30j	id-DGContent-DG10
EAC2_ISO7816_U_7k	EAC2_1.1	CMP.DG11	Compare DG11	AT_CERT_30k	id-DGContent-DG11
EAC2_ISO7816_U_7l	EAC2_1.1	CMP.DG12	Compare DG12	AT_CERT_30l	id-DGContent-DG12
EAC2_ISO7816_U_7m	EAC2_1.1	CMP.DG13	Compare DG13	AT_CERT_30m	id-DGContent-DG13
EAC2_ISO7816_U_7n	EAC2_1.1	CMP.DG14	Compare DG14	AT_CERT_30n	id-DGContent-DG14
EAC2_ISO7816_U_7o	EAC2_1.1	CMP.DG15	Compare DG15	AT_CERT_30o	id-DGContent-DG15
EAC2_ISO7816_U_7p	EAC2_1.1	CMP.DG16	Compare DG16	AT_CERT_30p	id-DGContent-DG16
EAC2_ISO7816_U_7q	EAC2_1.1	CMP.DG17	Compare DG17	AT_CERT_30q	id-DGContent-DG17
EAC2_ISO7816_U_7r	EAC2_1.1	CMP.DG18	Compare DG18	AT_CERT_30r	id-DGContent-DG18
EAC2_ISO7816_U_7s	EAC2_1.1	CMP.DG19	Compare DG19	AT_CERT_30s	id-DGContent-DG19
EAC2_ISO7816_U_7t	EAC2_1.1	CMP.DG20	Compare DG20	AT_CERT_30t	id-DGContent-DG20
EAC2_ISO7816_U_7u	EAC2_1.1	CMP.DG21	Compare DG21	AT_CERT_30u	id-DGContent-DG21
EAC2_ISO7816_U_7v	EAC2_1.1	CMP.DG22	Compare DG22	AT_CERT_30v	id-DGContent-DG22

Table 83: Test cases EAC2_ISO7816_U_7

3.15.8 Test case EAC2_ISO7816_U_8_Template

Test – ID	EAC2_ISO7816_U_8
Purpose	Negative test of Compare, verification fail because of empty tag 65 for Authentication Extension in MSE:Set AT during PACE
Version	EAC2_1.1
Profile	SMARTeID or eID, CMP, AUTH_EXT, required data group presence see table 84
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN and MSE:Set AT MUST contain an empty tag 65 without any data 2. The Terminal Authentication mechanism MUST have been performed with the certificates defined in “Certificate Set 30“ chapter as DV_CERT_30 and AT_CERT as defined in table 84

Test plan for eID-Cards with EAC 2.0

	<ul style="list-style-type: none"> 3. Compare data with valid data object as defined in table 84 MUST have been sent by authorized terminal during Terminal Authentication mechanism. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ul style="list-style-type: none"> 1. Send the given Compare APDU to the eID Card. '0C 33 00 00 <L_c> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the encrypted 'data object' as defined in table 84
Expected results	<ul style="list-style-type: none"> 1. Checking error in valid Secure Messaging response.

Test case EAC2_ISO7816_U_8a to test case EAC2_ISO7816_U_8v:

Testcase-ID	Version	Profile	Access Rules	Cert Reference	Data Object
EAC2_ISO7816_U_8a	EAC2_1.1	CMP.DG1	Compare DG1	AT_CERT_30a	id-DGContent-DG1
EAC2_ISO7816_U_8b	EAC2_1.1	CMP.DG2	Compare DG2	AT_CERT_30b	id-DGContent-DG2
EAC2_ISO7816_U_8c	EAC2_1.1	CMP.DG3	Compare DG3	AT_CERT_30c	id-DGContent-DG3
EAC2_ISO7816_U_8d	EAC2_1.1	CMP.DG4	Compare DG4	AT_CERT_30d	id-DGContent-DG4
EAC2_ISO7816_U_8e	EAC2_1.1	CMP.DG5	Compare DG5	AT_CERT_30e	id-DGContent-DG5
EAC2_ISO7816_U_8f	EAC2_1.1	CMP.DG6	Compare DG6	AT_CERT_30f	id-DGContent-DG6
EAC2_ISO7816_U_8g	EAC2_1.1	CMP.DG7	Compare DG7	AT_CERT_30g	id-DGContent-DG7
EAC2_ISO7816_U_8h	EAC2_1.1	CMP.DG8	Compare DG8	AT_CERT_30h	id-DGContent-DG8
EAC2_ISO7816_U_8i	EAC2_1.1	CMP.DG9	Compare DG9	AT_CERT_30i	id-DGContent-DG9
EAC2_ISO7816_U_8j	EAC2_1.1	CMP.DG10	Compare DG10	AT_CERT_30j	id-DGContent-DG10
EAC2_ISO7816_U_8k	EAC2_1.1	CMP.DG11	Compare DG11	AT_CERT_30k	id-DGContent-DG11
EAC2_ISO7816_U_8l	EAC2_1.1	CMP.DG12	Compare DG12	AT_CERT_30l	id-DGContent-DG12
EAC2_ISO7816_U_8m	EAC2_1.1	CMP.DG13	Compare DG13	AT_CERT_30m	id-DGContent-DG13
EAC2_ISO7816_U_8n	EAC2_1.1	CMP.DG14	Compare DG14	AT_CERT_30n	id-DGContent-DG14
EAC2_ISO7816_U_8o	EAC2_1.1	CMP.DG15	Compare DG15	AT_CERT_30o	id-DGContent-DG15
EAC2_ISO7816_U_8p	EAC2_1.1	CMP.DG16	Compare DG16	AT_CERT_30p	id-DGContent-DG16
EAC2_ISO7816_U_8q	EAC2_1.1	CMP.DG17	Compare DG17	AT_CERT_30q	id-DGContent-DG17
EAC2_ISO7816_U_8r	EAC2_1.1	CMP.DG18	Compare DG18	AT_CERT_30r	id-DGContent-DG18
EAC2_ISO7816_U_8s	EAC2_1.1	CMP.DG19	Compare DG19	AT_CERT_30s	id-DGContent-DG19
EAC2_ISO7816_U_8t	EAC2_1.1	CMP.DG20	Compare DG20	AT_CERT_30t	id-DGContent-DG20

Testcase-ID	Version	Profile	Access Rules	Cert Reference	Data Object
EAC2_ISO7816_U_8u	EAC2_1.1	CMP.DG21	Compare DG21	AT_CERT_30u	id-DGContent-DG21
EAC2_ISO7816_U_8v	EAC2_1.1	CMP.DG22	Compare DG22	AT_CERT_30v	id-DGContent-DG22

Table 84: Test cases EAC2_ISO7816_U_8**3.15.9 Test case EAC2_ISO7816_U_9**

Test – ID	EAC2_ISO7816_U_9
Purpose	Positive test of Compare command with two Discretionary Data Templates in Authentication Data Object containing age verification data and document validity verification data, verification successful, official domestic certificate
Version	EAC2_1.1
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification and document verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed with the certificates defined Certificate Set 17 chapter as DV_Cert_17 and AT_Cert_17j. 3. Auxiliary data with valid Date of Birth data object and document validity data object MUST have been sent by authorized terminal during Terminal Authentication mechanism. Date of birth and document validity MUST fit the required age and validity. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Compare APDU to the eID Card. '0C 33 00 00 <Lc> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth> 2. Send the given Compare APDU to the eID Card. '0C 33 00 00 <Lc> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-DateOfExpiry>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response.

3.15.10 Test case EAC2_ISO7816_U_10

Test – ID	EAC2_ISO7816_U_10
Purpose	Positive test with three Discretionary Data Templates in Authentication Data Object containing age verification data, document validity verification data and MunicipalityID verification data, verification successful, official domestic certificate

Test plan for eID-Cards with EAC 2.0

Version	EAC2_1.1
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification and document verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed with the certificates defined in Certificate Set 17 chapter as DV_Cert_17 and AT_Cert_17j. 3. Auxiliary data with valid Date of Birth data object, document validity data object and MunicipalityID data object MUST have been sent by authorized terminal during Terminal Authentication mechanism. Date of birth, document validity and MunicipalityID MUST fit the required age, validity and MunicipalityID. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Compare APDU to the eID Card. '0C 33 00 00 <Lc> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth> 2. Send the given Compare APDU to the eID Card. '0C 33 00 00 <Lc> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects: <id-DateOfExpiry> 3. Send the given Compare APDU to the eID Card. '0C 33 00 00 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' • <Cryptogram> contains the following encrypted data objects: <id-MunicipalityID>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response. 2. '90 00' within a valid Secure Messaging response. 3. '90 00' within a valid Secure Messaging response.

3.15.11 Test case EAC2_ISO7816_U_11

Test – ID	EAC2_ISO7816_U_11
Purpose	Positive test with two Discretionary Data Templates of the same type in Authentication Data Object containing two age verification data objects with same OID, verification of last data object successful, official domestic certificate
Version	EAC2_1.1
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification and document verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed with the certificates defined in Certificate Set 17 chapter as DV_Cert_17 and AT_Cert_17j.

	<p>AT_Cert_17j.</p> <ol style="list-style-type: none"> 3. Auxiliary data with two valid Date of Birth data objects MUST have been sent by authorized terminal during Terminal Authentication mechanism. The first date of birth MUST NOT fit the required age, the second date of birth MUST fit the required age. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Compare APDU to the eID Card. '0C 33 00 00 <Lc> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response.

3.15.12 Test case EAC2_ISO7816_U_12

Test – ID	EAC2_ISO7816_U_12
Purpose	Negative test with two Discretionary Data Templates of the same type in Authentication Data Object containing two age verification data objects with same OID, verification of last data object fail, official domestic certificate
Version	EAC2 1.1
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification and document verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed with the certificates defined in Certificate Set 17 chapter as DV_Cert_17 and AT_Cert_17j. 3. Auxiliary data with two valid Date of Birth data objects MUST have been sent by authorized terminal during Terminal Authentication mechanism. The first date of birth MUST fit the required age, the second date of birth MUST NOT fit the required age. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Compare APDU to the eID Card. '0C 33 00 00 <Lc> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth>
Expected results	<ol style="list-style-type: none"> 1. '63 40' or Checking error in a valid Secure Messaging response.

3.15.13 Test case EAC2_ISO7816_U_13

Test – ID	EAC2_ISO7816_U_13
-----------	-------------------

Test plan for eID-Cards with EAC 2.0

Purpose	Negative test with invalid Authentication Data Object containing an incorrect Discretionary Data Template tag
Version	EAC2_1.1
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification and document verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed with the certificates defined in Certificate Set 17 chapter as DV_Cert_17 and AT_Cert_17j. 3. Auxiliary data with invalid Date of Birth data objects MUST have been sent by authorized terminal during Terminal Authentication mechanism. The date of birth MUST fit the required age, but an incorrect tag 0x72 (instead of 0x73) is used. If the chip reacts at this step with a checking error, the following steps can be ignored and the chip has passed the test. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> 1. Send the given Compare APDU to the eID Card. '0C 33 00 00 <Lc> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth>
Expected results	<ol style="list-style-type: none"> 1. '6A 88' in a valid Secure Messaging response or checking error in step 3 of preconditions (in the last case the following steps and the test scenario cannot be performed).

3.15.14 Test case EAC2_ISO7816_U_14

Test – ID	EAC2_ISO7816_U_14
Purpose	Negative test with invalid Authentication Data Object containing an incorrect OID tag
Version	EAC2_1.1
Profile	SMARTeID or eID, AUX
Preconditions	<ol style="list-style-type: none"> 1. The PACE mechanism MUST have been performed using PIN, age verification and document verification must be allowed by CHAT 2. The Terminal Authentication mechanism MUST have been performed with the certificates defined in Certificate Set 17 chapter as DV_Cert_17 and AT_Cert_17j. 3. Auxiliary data with invalid Date of Birth data objects MUST have been sent by authorized terminal during Terminal Authentication mechanism. The first date of birth MUST fit the required age, but an incorrect tag 0x07 (instead of 0x06) for OID is used. If the chip reacts at this step with a checking error, the following steps can be ignored and the chip has passed the test. 4. The Chip Authentication MUST have been performed 5. The eID application MUST have been selected 6. All APDUs are sent as valid Secure Messaging APDUs

Test scenario	<ol style="list-style-type: none"> Send the given Compare APDU to the eID Card. '0C 33 00 00 <Lc> 85 <L₈₅> <Cryptogram> 8E 08 <Checksum> 00' <Cryptogram> contains the following encrypted data objects: <id-DateOfBirth>
Expected results	<ol style="list-style-type: none"> '6A 88' in a valid Secure Messaging response or checking error in step 3 of preconditions (in the last case the following steps and the test scenario cannot be performed).

3.16 Unit test EAC2_ISO7816_V_Chip Authentication Version 3

This version of the Chip Authentication is an alternative to Chip Authentication Version 2 combined with Restricted Identification providing also an authentication of the sector-specific identifier towards the terminal and the pseudonymity of the eIDAS token without the need to use the same keys on several chips. Cryptographically, the protocol is based on the combination of an ephemeral key agreement with a Pseudonymous Signature (PS).

The EF.CardSecurity file may contain an optional key reference identifier. This is useful if the chip supports multiple keys for Chip Authentication. The MSE:Set AT command can be called either with implicit key selection if no key reference is included in EF.CardSecurity or with the explicit key reference defined in the EF.CardSecurity element. All tests in this unit SHOULD be used with implicit or explicit key reference depending on the presence of the key reference element in EF.CardSecurity.

The EF.CardSecurity may contain more than one ChipAuthenticationPublicKeyInfo. In this case, all appropriate tests MUST be performed for each key. The corresponding test case is only rated as a PASS if all test case runs are completed successfully. For test cases where the Chip Authentication mechanism is just used as precondition the first key is always used.

The tests defined in this test unit shall be run once. In Preconditions and otherwise specified, Terminal Authentication version 2 SHALL be performed with the certificates DV_CERT_17 and AT_CERT_17i.

The eIDAS token MAY return up to two sector-specific pseudonyms during execution of the Pseudonymous Signature Authentication (PSA). In the appropriate test cases of this Unit, the generation and output of each pseudonym shall conform to the PSAInfo information provided in the ICS. If not, the step of the scenario shall fail.

3.16.1 Test case EAC2_ISO7816_V_1

Test – ID	EAC2 ISO7816 V 1
Purpose	Positive test: Perform Chip Authentication Version 3 with MSE: Set AT / General Authenticate commands
Version	EAC2 1.1
Profile	eID, CA3
Preconditions	<ol style="list-style-type: none"> Perform PACE with Generic Mapping Terminal Authentication Version 2 must be performed Extract ChipAuthenticationPublicKeyInfo from EF.CardSecurity and generate an ephemeral key pair
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <CA OID> 84 <L₈₄> <private key reference>'

	<p>within Secure Messaging. The private key reference MUST be included in the APDU specified in the ChipAuthenticationInfo structure stored in the file EF.CardSecurity</p> <ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token: '00 86 00 00 <L_c> 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> <L_e>' within Secure Messaging 3. Restart Secure Messaging with new derived session keys 4. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <PSA OID> 84 <L₈₄> <private key reference>' within Secure Messaging 5. Compute Pseudonymous Signature with ephemeral public key as input. Perform Pseudonymous Signature Authentication with computed signature: '00 86 00 00 <L_c> 7C <L_{7C}> 80 <L₈₀> <sector public key> <L_e>' within Secure Messaging
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. '7C <L_{7C}> 81 <L₈₁> <Public Key> 90 00' in a valid Secure Messaging response 3. - 4. '90 00' within a valid Secure Messaging response 5. '7C <L_{7C}> 82 <L₈₂> <First Pseudonym Public Key> 83 <L₈₃> <Second Pseudonym Public Key> 84 <L₈₄> <Pseudonymous Signature> 90 00' in a valid Secure Messaging response. <p>The presence of Tag 82 and Tag 83 shall be coherent with the ICS</p>

3.16.2 Test case EAC2_ISO7816_V_2

Test – ID	EAC2 ISO7816 V 2
Purpose	<p>Positive test: Perform Chip Authentication Version 3 with MSE: Set AT / General Authenticate commands</p> <p>The ephemeral PACE-GM Public key shall be reused by the chip. If not, the test is not applicable</p>
Version	EAC2_1.1
Profile	eID, CA3_ReUse
Preconditions	<ol style="list-style-type: none"> 1. ECDH Domain parameters between PACE-GM and CA3 must be identical 2. Perform PACE with Generic Mapping 3. Terminal Authentication Version 2 must be performed 4. Extract ChipAuthenticationPublicKeyInfo from EF.CardSecurity and generate an ephemeral key pair
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <CA OID> 84 <L₈₄> <private key reference>' within Secure Messaging. The private key reference MUST be included in the

	<p>APDU specified in the ChipAuthenticationInfo structure stored in EF.CardSecurity file</p> <ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token: '00 86 00 00 <L_c> 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> <L_e>' within Secure Messaging 3. Restart Secure Messaging with new derived session keys 4. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <PSA OID> 84 <L₈₄> <private key reference>' within Secure Messaging 5. Compute Pseudonymous Signature with ephemeral public key as input. Use the ephemeral public key of PACE mapping (GM) as ephemeral public key. Perform Pseudonymous Signature Authentication with computed signature: '00 86 00 00 <L_c> 7C <L_{7C}> 80 <L₈₀> <sector public key> <L_e>' within Secure Messaging
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. '7C <L_{7C}> 81 <L₈₁> <Public Key> 90 00' in a valid Secure Messaging response. The Public Key shall be identical to the one sent during the step 2 of PACE GM mechanism 3. - 4. '90 00' within a valid Secure Messaging response 5. '7C <L_{7C}> 82 <L₈₂> <First Pseudonym Public Key> 83 <L₈₃> <Second Pseudonym Public Key> 84 <L₈₄> <Pseudonymous Signature> 90 00' in a valid Secure Messaging response. <p>The presence of Tag 82 and Tag 83 shall be coherent with the ICS</p>

3.16.3 Test case EAC2_ISO7816_V_3

Test – ID	EAC2_ISO7816_V_3
Purpose	Negative test: Perform Pseudonymous Signature command with a valid ephemeral public key, but without Secure Messaging
Version	EAC2 1.1
Profile	eID, CA3
Preconditions	<ol style="list-style-type: none"> 1. Perform PACE with Generic Mapping 2. Terminal Authentication Version 2 must be performed 3. Extract ChipAuthenticationPublicKeyInfo from EF.CardSecurity and generate an ephemeral key pair
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <CA OID> 84 <L₈₄> <private key reference>' within Secure Messaging. The private key reference MUST be included in the APDU specified in the ChipAuthenticationInfo structure stored in

Test plan for eID-Cards with EAC 2.0

	<p>EF.CardSecurity file</p> <ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token: '00 86 00 00 <L_c> 7C <L_{7c}> 80 <L₈₀> <ephemeral public key> <L_e>' within Secure Messaging 3. Restart Secure Messaging with new derived session keys 4. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <PSA OID> 84 <L₈₄> <private key reference>' within Secure Messaging 5. Compute Pseudonymous Signature with ephemeral public key as input. Perform Pseudonymous Signature Authentication with computed signature: '00 86 00 00 <L_c> 7C <L_{7c}> 80 <L₈₀> <sector public key> <L_e>' without Secure Messaging
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. '7C <L_{7c}> 81 <L₈₁> <Public Key> 90 00' in a valid Secure Messaging response 3. - 4. '90 00' within a valid Secure Messaging response 5. Checking error or Execution error or Warning in plain response

3.16.4 Test case EAC2_ISO7816_V_4

Test – ID	EAC2 ISO7816 V 4
Purpose	Negative test: Perform Pseudonymous Signature command with a valid ephemeral public key, but with invalid data object tag for the sector public key.
Version	EAC2 1.1
Profile	eID, CA3
Preconditions	<ol style="list-style-type: none"> 1. Perform PACE with Generic Mapping 2. Terminal Authentication Version 2 must be performed 3. Extract ChipAuthenticationPublicKeyInfo from EF.CardSecurity and generate an ephemeral key pair
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <CA OID> 84 <L₈₄> <private key reference>' within Secure Messaging. The private key reference MUST be included in the APDU specified in the ChipAuthenticationInfo structure stored in EF.CardSecurity file 2. Send the given General Authenticate APDU to the eIDAS token: '00 86 00 00 <L_c> 7C <L_{7c}> 80 <L₈₀> <ephemeral public key> <L_e>' within Secure Messaging 3. Restart Secure Messaging with new derived session keys

	<p>4. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <PSA OID> 84 <L₈₄> <private key reference>' within Secure Messaging</p> <p>5. Compute Pseudonymous Signature with ephemeral public key as input. Perform Pseudonymous Signature Authentication with computed signature, using a wrong tag (84 instead of 80): '00 86 00 00 <L_c> 7C <L_{7C}> 84 <L₈₄> <sector public key> <L_e>' within Secure Messaging</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. '7C <L_{7C}> 81 <L₈₁> <Public Key> 90 00' in a valid Secure Messaging response 3. - 4. '90 00' within a valid Secure Messaging response 5. Checking error or Execution error or Warning in valid Secure Messaging response

3.16.5 Test case EAC2_ISO7816_V_5

Test – ID	EAC2_ISO7816_V_5
Purpose	Negative test: Perform Pseudonymous Signature command with a valid ephemeral public key, but with missing sector public key
Version	EAC2 1.1
Profile	eID, CA3
Preconditions	<ol style="list-style-type: none"> 1. Perform PACE with Generic Mapping 2. Terminal Authentication Version 2 must be performed 3. Extract ChipAuthenticationPublicKeyInfo from EF.CardSecurity and generate an ephemeral key pair
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <CA OID> 84 <L₈₄> <private key reference>' within Secure Messaging. The private key reference MUST be included in the APDU specified in the ChipAuthenticationInfo structure stored in EF.CardSecurity file</p> <p>2. Send the given General Authenticate APDU to the eIDAS token: '00 86 00 00 <L_c> 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> <L_e>' within Secure Messaging</p> <p>3. Restart Secure Messaging with new derived session keys</p> <p>4. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <PSA OID> 84 <L₈₄> <private key reference>' within Secure Messaging</p>

	<p>5. Compute Pseudonymous Signature with ephemeral public key as input. Perform Pseudonymous Signature Authentication with computed signature but missing sector public key: '00 86 00 00 <L_c> 7C 00 <L_e>' within Secure Messaging</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. '7C <L_{7C}> 81 <L₈₁> <Public Key> 90 00' in a valid Secure Messaging response 3. - 4. '90 00' within a valid Secure Messaging response 5. Checking error or Execution error or Warning in valid Secure Messaging response

3.16.6 Test case EAC2_ISO7816_V_6

Test – ID	EAC2 ISO7816 V 6
Purpose	Negative test: Perform Pseudonymous Signature command with a valid ephemeral public key, but with an empty sector public key
Version	EAC2 1.1
Profile	eID, CA3
Preconditions	<ol style="list-style-type: none"> 1. Perform PACE with Generic Mapping 2. Terminal Authentication Version 2 must be performed 3. Extract ChipAuthenticationPublicKeyInfo from EF.CardSecurity and generate an ephemeral key pair
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <CA OID> 84 <L₈₄> <private key reference>' within Secure Messaging. The private key reference MUST be included in the APDU specified in the ChipAuthenticationInfo structure stored in EF.CardSecurity file 2. Send the given General Authenticate APDU to the eIDAS token: '00 86 00 00 <L_c> 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> <L_e>' within Secure Messaging 3. Restart Secure Messaging with new derived session keys 4. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <PSA OID> 84 <L₈₄> <private key reference>' within Secure Messaging 5. Compute Pseudonymous Signature with ephemeral public key as input. Perform Pseudonymous Signature Authentication with computed signature but empty sector public key: '00 86 00 00 <L_c> 7C 03 80 01 00 <L_e>' within Secure Messaging

Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. '7C <L_{7C}> 81 <L₈₁> <Public Key> 90 00' in a valid Secure Messaging response 3. - 4. '90 00' within a valid Secure Messaging response 5. Checking error or Execution error or Warning in valid Secure Messaging response
------------------	--

3.16.7 Test case EAC2_ISO7816_V_7

Test – ID	EAC2_ISO7816_V_7
Purpose	Negative test: Perform Chip Authentication Version 3 of the Anonymous Diffie-Hellman in the first part, but with old session keys during the Pseudonymous Signature Authentication
Version	EAC2 1.1
Profile	eID, CA3
Preconditions	<ol style="list-style-type: none"> 1. Perform PACE with Generic Mapping 2. Terminal Authentication Version 2 must be performed 3. Extract ChipAuthenticationPublicKeyInfo from EF.CardSecurity and generate an ephemeral key pair
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <CA OID> 84 <L₈₄> <private key reference>' within Secure Messaging. The private key reference MUST be included in the APDU specified in the ChipAuthenticationInfo structure stored in EF.CardSecurity file 2. Send the given General Authenticate APDU to the eIDAS token: '00 86 00 00 <L_c> 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> <L_e>' within Secure Messaging 3. Do not restart Secure Messaging and send the given MSE: Set AT APDU with old SM keys to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <PSA OID> 84 <L₈₄> <private key reference>' within secure messaging (old SM keys)
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. '7C <L_{7C}> 81 <L₈₁> <Public Key> 90 00' in a valid Secure Messaging response 3. Checking error or Execution error or Warning in plain

3.16.8 Test case EAC2_ISO7816_V_8

Test – ID	EAC2_ISO7816_V_8
Purpose	Negative test: Perform Chip Authentication Version 3 with a public key in the first General Authenticate command that does not match the compressed public key sent during Terminal Authentication

Test plan for eID-Cards with EAC 2.0

Version	EAC2_1.1
Profile	eID, CA3
Preconditions	<ol style="list-style-type: none"> 1. Perform PACE with Generic Mapping 2. Terminal Authentication Version 2 must be performed 3. Extract ChipAuthenticationPublicKeyInfo from EF.CardSecurity and generate an ephemeral key pair
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <CA OID> 84 <L₈₄> <private key reference>' within secure messaging. The private key reference MUST be included in the APDU specified in the ChipAuthenticationInfo structure stored in EF.CardSecurity file 2. Send the given General Authenticate APDU to the eIDAS token: '00 86 00 00 <L_c> 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> <L_e>' within Secure Messaging. Use an ephemeral public key that does not match to the compressed public key sent in Terminal Authentication
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. Checking error or Execution error or Warning in valid Secure Messaging response

3.16.9 Test case EAC2_ISO7816_V_9

Test – ID	EAC2_ISO7816_V_9
Purpose	Negative test: Perform Chip Authentication Version 3 with a public key in the first General Authenticate command that is not on the curve
Version	EAC2_1.1
Profile	eID, CA3
Preconditions	<ol style="list-style-type: none"> 1. Perform PACE with Generic Mapping 2. Terminal Authentication Version 2 must be performed 3. Extract ChipAuthenticationPublicKeyInfo from EF.CardSecurity and generate an ephemeral key pair
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <CA OID> 84 <L₈₄> <private key reference>' within secure messaging. The private key reference MUST be included in the APDU specified in the ChipAuthenticationInfo structure stored in EF.CardSecurity file 2. Send the given General Authenticate APDU to the eIDAS token: '00 86 00 00 <L_c> 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> <L_e>' within Secure Messaging. Use an ephemeral public key that does not belong to the curve.
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response

	2. Checking error or Execution error or Warning in valid Secure Messaging response
--	--

3.16.10 Test case EAC2_ISO7816_V_10

Test – ID	EAC2_ISO7816_V_10
Purpose	Negative test: Perform Chip Authentication Version 3 without Anonymous Diffie-Hellman key agreement before Pseudonymous Signature Authentication.
Version	EAC2_1.1
Profile	eID, CA3
Preconditions	<ol style="list-style-type: none"> 1. Perform PACE with Generic Mapping 2. Terminal Authentication Version 2 must be performed 3. Extract ChipAuthenticationPublicKeyInfo from EF.CardSecurity and generate an ephemeral key pair
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <CA OID> 84 <L₈₄> <private key reference>' within secure messaging. 2. Compute Pseudonymous Signature. Perform Pseudonymous Signature Authentication with computed signature: '00 86 00 00 <L_c> 7C <L_{7C}> 80 <L₈₀> <sector public key> <L_c>' within secure messaging
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. If CA2 is NOT supported: Checking error or Execution error or Warning in valid Secure Messaging response If CA2 is supported: '90 00' in a valid Secure Messaging response

3.16.11 Test case EAC2_ISO7816_V_11

Test – ID	EAC2_ISO7816_V_11
Purpose	Positive test: Perform Chip Authentication Version 3 commands in an unusual sequence: commands of ADH are performed once and commands of PSA are performed a second time
Version	EAC2_1.1
Profile	eID, CA3
Preconditions	<ol style="list-style-type: none"> 1. Perform PACE with Generic Mapping 2. Terminal Authentication Version 2 must be performed 3. Extract ChipAuthenticationPublicKeyInfo from EF.CardSecurity and generate an ephemeral key pair
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <CA OID> 84 <L₈₄> <private key reference>' within Secure Messaging. The private key reference MUST be included in the APDU specified in the ChipAuthenticationInfo structure stored in

Test plan for eID-Cards with EAC 2.0

	<p>EF.CardSecurity</p> <ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token: '00 86 00 00 <L_c> 7C <L_{7c}> 80 <L₈₀> <ephemeral public key> <L_e>' within Secure Messaging 3. Restart Secure Messaging with new derived session keys 4. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <PSA OID> 84 <L₈₄> <private key reference>' within Secure Messaging 5. Compute Pseudonymous Signature with a correct ephemeral public key as input. Perform Pseudonymous Signature Authentication with computed signature: '00 86 00 00 <L_c> 7C <L_{7c}> 80 <L₈₀> <sector public key> <L_e>' within Secure Messaging 6. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <PSA OID> 84 <L₈₄> <private key reference>' within Secure Messaging 7. Compute Pseudonymous Signature with a correct ephemeral public key as input. Perform Pseudonymous Signature Authentication with computed signature: '00 86 00 00 <L_c> 7C <L_{7c}> 80 <L₈₀> <sector public key> <L_e>' within Secure Messaging
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. '7C <L_{7c}> 81 <L₈₁> <Public Key> 90 00' in a valid Secure Messaging response 3. - 4. '90 00' within a valid Secure Messaging response 5. '7C <L_{7c}> 82 <L₈₂> <First Pseudonym Public Key> 83 <L₈₃> <Second Pseudonym Public Key> 84 <L₈₄> <Pseudonymous Signature> 90 00' in a valid Secure Messaging response. The presence of Tag 82 and Tag 83 shall be coherent with the ICS 6. '90 00' within a valid Secure Messaging response 7. '7C <L_{7c}> 82 <L₈₂> <First Pseudonym Public Key> 83 <L₈₃> <Second Pseudonym Public Key> 84 <L₈₄> <Pseudonymous Signature> 90 00' in a valid Secure Messaging response. The presence of Tag 82 and Tag 83 shall be coherent with the ICS

3.16.12 Test case EAC2_ISO7816_V_12

Test – ID	EAC2_ISO7816_V_12
Purpose	Negative test: Perform Chip Authentication Version 3 commands where PSA is using a sector-specific key that does not match to the hash of the certificate extension

Version	EAC2_1.1
Profile	eID, CA3
Preconditions	<ol style="list-style-type: none"> 1. Perform PACE with Generic Mapping 2. Terminal Authentication Version 2 must be performed 3. Extract ChipAuthenticationPublicKeyInfo from EF.CardSecurity and generate an ephemeral key pair
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <CA OID> 84 <L₈₄> <private key reference>' within Secure Messaging. The private key reference MUST be included in the APDU specified in the ChipAuthenticationInfo structure stored in EF.CardSecurity file 2. Send the given General Authenticate APDU to the eIDAS token: '00 86 00 00 <L_c> 7C <L_{7C}> 80 <L₈₀> <ephemeral public key> <L_e>' within Secure Messaging 3. Restart Secure Messaging with new derived session keys 4. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 41 A4 <L_c> 80 <L₈₀> <PSA OID> 84 <L₈₄> <private key reference>' within Secure Messaging 5. Compute Pseudonymous Signature with a correct ephemeral public key as input. Perform Pseudonymous Signature Authentication with computed signature. Use a sector-specific key that does not match to hash of certificate extension: '00 86 00 00 <L_c> 7C <L_{7C}> 80 <L₈₀> <sector public key> <L_e>' within Secure Messaging
Expected results	<ol style="list-style-type: none"> 1. '90 00' within a valid Secure Messaging response 2. '7C <L_{7C}> 81 <L₈₁> <Public Key> 90 00' in a valid Secure Messaging response 3. - 4. '90 00' within a valid Secure Messaging response 5. 'Checking error or Execution error or Warning in valid Secure Messaging response'

3.17 Unit test EAC2_ISO7816_W_Initial External Authentication (IEA)

The protocol Initial External Authentication is used to assure a binding between device application (e.g. smartphone app) and secure element of the corresponding device. It is introduced in context of Smart-eID and the protocol is specified in [12].

3.17.1 Test case EAC2_ISO7816_W_1

Test – ID	EAC2 ISO7816 W 1
Purpose	Positive test: Perform Initial External Authentication
Version	EAC2 1.3
Profile	SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 81 A4 <L_c> 83 <L₈₃> <public key reference>' in plain. The public key reference for PuK.IEA MUST be included in the APDU specified in the ICS as valid key for IEA. 2. Send the given Get Challenge APDU to the eIDAS token: '00 84 00 00 08' in plain. 3. Send the given External Authenticate APDU to the eIDAS token: '00 82 00 00 <L_c> <data>' in plain. The <data> MUST be calculated from the given IEA private key and the challenge returned in step 2 (SIGN(RND.ICC, PrK.IEA) with ECDSA).
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. The eIDAS token MUST return 8 random bytes and the status bytes '90 00' in plain. 3. '90 00' in plain

3.17.2 Test case EAC2_ISO7816_W_2

Test – ID	EAC2 ISO7816 W 2
Purpose	Positive test: Perform Initial External Authentication with two challenges and use the second one
Version	EAC2 1.3
Profile	SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 81 A4 <L_c> 83 <L₈₃> <public key reference>' in plain. The public key reference for PuK.IEA MUST be included in the APDU specified in the ICS as valid key for IEA.

	<ol style="list-style-type: none"> 2. Send the given Get Challenge APDU to the eIDAS token: '00 84 00 00 08' in plain. 3. Send the given Get Challenge APDU to the eIDAS token: '00 84 00 00 08' in plain. 4. Send the given External Authenticate APDU to the eIDAS token: '00 82 00 00 <Lc> <data>' in plain. The <data> MUST be calculated from the given IEA private key and the challenge returned in step 3 (SIGN(RND.ICC, PrK.IEA) with ECDSA).
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. The eIDAS token MUST return 8 random bytes and the status bytes '90 00' in plain. 3. The eIDAS token MUST return 8 random bytes and the status bytes '90 00' in plain. 4. '90 00' in plain

3.17.3 Test case EAC2_ISO7816_W_3

Test – ID	EAC2_ISO7816_W_3
Purpose	Negative test: Perform Initial External Authentication with invalid key reference.
Version	EAC2 1.3
Profile	SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 81 A4 <Lc> 83 <L83> <public key reference>' in plain. The public key reference for PuK.IEA MUST be included in the APDU specified in the ICS as an invalid key for IEA. 2. Send the given Get Challenge APDU to the eIDAS token: '00 84 00 00 08' in plain. 3. Send the given External Authenticate APDU to the eIDAS token: '00 82 00 00 <Lc> <data>' in plain. The <data> MUST be calculated from the given IEA private key and the challenge returned in step 2 (SIGN(RND.ICC, PrK.IEA) with ECDSA).
Expected results	<ol style="list-style-type: none"> 1. Checking Error or '90 00' in plain. In case of Checking error, step 2 and step 3 can be canceled. 2. The eIDAS token MUST return 8 random bytes and the status bytes '90 00' in plain. 3. Checking Error in plain

3.17.4 Test case EAC2_ISO7816_W_4

Test – ID	EAC2_ISO7816_W_4
Purpose	Negative test: Perform Initial External Authentication with missing key reference.
Version	EAC2 1.3
Profile	SMARTeID
Preconditions	<ul style="list-style-type: none"> 1. None, card recently activated
Test scenario	<ul style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 81 A4' in plain. The public key reference is missing. 2. Send the given Get Challenge APDU to the eIDAS token: '00 84 00 00 08' in plain. 3. Send the given External Authenticate APDU to the eIDAS token: '00 82 00 00 <L_c> <data>' in plain. The <data> MUST be calculated from the given IEA private key and the challenge returned in step 2 (SIGN(RND.ICC, PrK.IEA) with ECDSA).
Expected results	<ul style="list-style-type: none"> 1. Checking Error or '90 00' in plain. In case of Checking error, step 2 and step 3 can be canceled. 2. The eIDAS token MUST return 8 random bytes and the status bytes '90 00' in plain. 3. Checking Error in plain

3.17.5 Test case EAC2_ISO7816_W_5

Test – ID	EAC2_ISO7816_W_5
Purpose	Negative test: Perform Initial External Authentication with wrong key reference tag ('84' instead of '83')
Version	EAC2 1.3
Profile	SMARTeID
Preconditions	<ul style="list-style-type: none"> 1. None, card recently activated
Test scenario	<ul style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 81 A4 <L_c> 84 <L₈₄> <public key reference>' in plain. The public key reference for PuK.IEA MUST be included in the APDU specified in the ICS as valid key for IEA but the tag '84' is wrong. 2. Send the given Get Challenge APDU to the eIDAS token: '00 84 00 00 08' in plain. 3. Send the given External Authenticate APDU to the eIDAS token: '00 82 00 00 <L_c> <data>' in plain. The <data> MUST be calculated from the given IEA private key and the challenge returned in step 2 (SIGN(RND.ICC, PrK.IEA) with ECDSA).

Expected results	<ol style="list-style-type: none"> 1. Checking Error or '90 00' in plain. In case of Checking error, step 2 and step 3 can be canceled. 2. The eIDAS token MUST return 8 random bytes and the status bytes '90 00' in plain. 3. Checking Error in plain
------------------	--

3.17.6 Test case EAC2_ISO7816_W_6

Test – ID	EAC2_ISO7816_W_6
Purpose	Negative test: Perform Initial External Authentication with command chaining what is not allowed here (command GET CHALLENGE).
Version	EAC2_1.3
Profile	SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 81 A4 <L_c> 83 <L₈₃> <public key reference>' in plain. The public key reference for PuK.IEA MUST be included in the APDU specified in the ICS as valid key for IEA but the tag '84' is wrong. 2. Send the given Get Challenge APDU to the eIDAS token: '10 84 00 00 08' in plain.
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain. 2. Checking Error in plain.

3.17.7 Test case EAC2_ISO7816_W_7

Test – ID	EAC2_ISO7816_W_7
Purpose	Negative test: Perform Initial External Authentication with too long challenge
Version	EAC2_1.3
Profile	SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 81 A4 <L_c> 83 <L₈₃> <public key reference>' in plain. The public key reference for PuK.IEA MUST be included in the APDU specified in the ICS as valid key for IEA. 2. Send the given Get Challenge APDU to the eIDAS token: '00 84 00 00 09' in plain. 3. Send the given External Authenticate APDU to the eIDAS token: '00 82 00 00 <L_c> <data>' in plain. The <data> MUST be calculated from the given IEA private key and

Test plan for eID-Cards with EAC 2.0

	the too long challenge returned in step 2 (SIGN(RND.ICC, PrK.IEA) with ECDSA).
Expected results	<ol style="list-style-type: none"> 1. ‘90 00’ in plain 2. The eIDAS token MUST return 9 random bytes and the status bytes ‘90 00’ in plain or ‘67 00’ in case that eIDAS token don’t support challenges != 8. In case of ‘67 00’ step 3 can be skipped. 3. Checking Error in plain

3.17.8 Test case EAC2_ISO7816_W_8

Test – ID	EAC2_ISO7816_W_8
Purpose	Negative test: Perform Initial External Authentication with too short challenge
Version	EAC2_1.3
Profile	SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: ‘00 22 81 A4 <L_c> 83 <L₈₃> <public key reference>’ in plain. The public key reference for PuK.IEA MUST be included in the APDU specified in the ICS as valid key for IEA. 2. Send the given Get Challenge APDU to the eIDAS token: ‘00 84 00 00 07’ in plain. 3. Send the given External Authenticate APDU to the eIDAS token: ‘00 82 00 00 <L_c> <data>’ in plain. The <data> MUST be calculated from the given IEA private key and the too short challenge returned in step 2 (SIGN(RND.ICC, PrK.IEA) with ECDSA).
Expected results	<ol style="list-style-type: none"> 1. ‘90 00’ in plain 2. The eIDAS token MUST return 7 random bytes and the status bytes ‘90 00’ in plain or ‘67 00’ in case that eIDAS token don’t support challenges != 8. In case of ‘67 00’ step 3 can be skipped. 3. Checking Error in plain

3.17.9 Test case EAC2_ISO7816_W_9

Test – ID	EAC2_ISO7816_W_9
Purpose	Negative test: Perform Initial External Authentication with no data in External Authenticate command.
Version	EAC2_1.3
Profile	SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token:

	<p>'00 22 81 A4 <L_c> 83 <L₈₃> <public key reference>' in plain. The public key reference for PuK.IEA MUST be included in the APDU specified in the ICS as valid key for IEA.</p> <ol style="list-style-type: none"> 2. Send the given Get Challenge APDU to the eIDAS token: '00 84 00 00 08' in plain. 3. Send the given External Authenticate APDU to the eIDAS token: '00 82 00 00' in plain.
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. The eIDAS token MUST return 8 random bytes and the status bytes '90 00' in plain. 3. Checking Error in plain

3.17.10 Test case EAC2_ISO7816_W_10

Test – ID	EAC2_ISO7816_W_10
Purpose	Negative test: Perform Initial External Authentication with empty data in External Authenticate command.
Version	EAC2 1.3
Profile	SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 81 A4 <L_c> 83 <L₈₃> <public key reference>' in plain. The public key reference for PuK.IEA MUST be included in the APDU specified in the ICS as valid key for IEA. 2. Send the given Get Challenge APDU to the eIDAS token: '00 84 00 00 08' in plain. 3. Send the given External Authenticate APDU to the eIDAS token: '00 82 00 00 01 00' in plain.
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. The eIDAS token MUST return 8 random bytes and the status bytes '90 00' in plain. 3. Checking Error in plain

3.17.11 Test case EAC2_ISO7816_W_11

Test – ID	EAC2_ISO7816_W_11
Purpose	Negative test: Perform Initial External Authentication with incorrect challenge in External Authenticate command.

Test plan for eID-Cards with EAC 2.0

Version	EAC2_1.3
Profile	SMARTeID
Preconditions	1. None, card recently activated
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 81 A4 <L_c> 83 <L₈₃> <public key reference>' in plain. The public key reference for PuK.IEA MUST be included in the APDU specified in the ICS as valid key for IEA.</p> <p>2. Send the given Get Challenge APDU to the eIDAS token: '00 84 00 00 08' in plain.</p> <p>3. Send the given External Authenticate APDU to the eIDAS token: '00 82 00 00 <L_c> <data>' in plain. The <data> MUST be calculated from the given IEA private key and a challenge different from the one returned in step 2 (SIGN(RND.ICC, PrK.IEA) with ECDSA).</p>
Expected results	<p>1. '90 00' in plain</p> <p>2. The eIDAS token MUST return 8 random bytes and the status bytes '90 00' in plain.</p> <p>3. '63 00' or Checking Error in plain</p>

3.17.12 Test case EAC2_ISO7816_W_12

2Test – ID	EAC2_ISO7816_W_12
Purpose	Negative test: Perform Initial External Authentication with invalid signing algorithm.
Version	EAC2_1.3
Profile	SMARTeID
Preconditions	1. None, card recently activated
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 81 A4 <L_c> 83 <L₈₃> <public key reference>' in plain. The public key reference for PuK.IEA MUST be included in the APDU specified in the ICS as valid key for IEA.</p> <p>2. Send the given Get Challenge APDU to the eIDAS token: '00 84 00 00 08' in plain.</p> <p>3. Send the given External Authenticate APDU to the eIDAS token: '00 82 00 00 <L_c> <data>' in plain. The <data> MUST be calculated from the given IEA private key and the challenge returned in step 2 (SIGN(RND.ICC, PrK.IEA) with an invalid alternative to referenced ECDSA algorithm).</p>
Expected results	<p>1. '90 00' in plain</p> <p>2. The eIDAS token MUST return 8 random bytes and the status bytes '90 00' in plain.</p> <p>3. '63 00' or Checking Error in plain</p>

3.17.13 Test case EAC2_ISO7816_W_13

Test – ID	EAC2_ISO7816_W_13
Purpose	Negative test: Perform Initial External Authentication with command chaining what is not allowed here (command EXTERNAL AUTHENTICATE).
Version	EAC2_1.3
Profile	SMARTeID
Preconditions	1. None, card recently activated
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 81 A4 <L_c> 83 <L₈₃> <public key reference>' in plain. The public key reference for PuK.IEA MUST be included in the APDU specified in the ICS as valid key for IEA but the tag '84' is wrong.</p> <p>2. Send the given Get Challenge APDU to the eIDAS token: '00 84 00 00 08' in plain.</p> <p>3. Send the given External Authenticate APDU to the eIDAS token: '10 82 00 00 <L_c> <data>' in plain. The <data> MUST be calculated from the given IEA private key and the challenge returned in step 2 (SIGN(RND.ICC, PrK.IEA) with ECDSA).</p>
Expected results	<p>1. '90 00' in plain.</p> <p>2. '90 00' in plain.</p> <p>3. Checking Error in plain</p>

3.17.14 Test case EAC2_ISO7816_W_14

Test – ID	EAC2_ISO7816_W_14
Purpose	Negative test: Perform Initial External Authentication without challenge delivered by chip
Version	EAC2_1.3
Profile	SMARTeID
Preconditions	1. None, card recently activated
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 81 A4 <L_c> 83 <L₈₃> <public key reference>' in plain. The public key reference for PuK.IEA MUST be included in the APDU specified in the ICS as valid key for IEA.</p> <p>2. Send the given External Authenticate APDU to the eIDAS token: '00 82 00 00 <L_c> <data>' in plain. The <data> MUST be calculated only from the given IEA private key (SIGN(PrK.IEA) with ECDSA).</p>
Expected results	<p>1. '90 00' in plain.</p> <p>2. Checking Error in plain.</p>

3.17.15 Test case EAC2_ISO7816_W_15

Test – ID	EAC2_ISO7816_W_15
Purpose	Negative test: Perform Initial External Authentication with two challenges and use the first one
Version	EAC2_1.3
Profile	SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token: '00 22 81 A4 <L_c> 83 <L₈₃> <public key reference>' in plain. The public key reference for PuK.IEA MUST be included in the APDU specified in the ICS as valid key for IEA. 2. Send the given Get Challenge APDU to the eIDAS token: '00 84 00 00 08' in plain. 3. Send the given Get Challenge APDU to the eIDAS token: '00 84 00 00 08' in plain. 4. Send the given External Authenticate APDU to the eIDAS token: '00 82 00 00 <L_c> <data>' in plain. The <data> MUST be calculated from the given IEA private key and the challenge returned in step 2 (SIGN(RND.ICC, PrK.IEA) with ECDSA).
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. The eIDAS token MUST return 8 random bytes and the status bytes '90 00' in plain. 3. The eIDAS token MUST return 8 random bytes and the status bytes '90 00' in plain. 4. '63 00' or Checking error in plain

3.18 Unit test EAC2_ISO7816_X_CA+PA

The protocol CA+PA aka PACE-light is introduced as an alternative to PACE for secure elements which lack the support for point addition on elliptic curves introduced by standard PACE protocol. CAPA is introduced in context of Smart-eID and the protocol is specified in [12].

All test cases of this unit MUST be executed for each CA+PA protocol indicated in the CAPAInfo elements present in EF.CardAccess of the eID. Preconditions MUST be run with each CAPAInfo element.

3.18.1 Test case EAC2_ISO7816_X_1

Test – ID	EAC2_ISO7816_X_1
Purpose	Positive test: Perform CAPA without CHAT
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ul style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: <code>'00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>'</code> <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: <code>'10 86 00 00 <L_c> 7C 00 <L_e>'</code> 3. Send the given General Authenticate APDU to the eIDAS token without data: <code>'10 86 00 00 <L_c> 7C 02 81 00 <L_e>'</code> 4. Perform key agreement: <code>'10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>'</code> 5. Perform explicit authentication: <code>'00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'</code> 6. Perform explicit verification (VERIFY command) with Secure Messaging: <code>'00 20 00 03 <L_c> <PIN>'</code>
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain

Test plan for eID-Cards with EAC 2.0

	<ol style="list-style-type: none"> 5. $7C <L_{7C}> 86 <L_{86}> <MAC(PuK.IFD.DH, K.MAC)>$ and SW '90 00' in plain 6. '90 00' within a valid SM response
--	---

3.18.2 Test case EAC2_ISO7816_X_2

Test – ID	EAC2 ISO7816 X 2
Purpose	Positive test: Perform CAPA with CHAT
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: $'00 22 81 A4 <L_c> 80 <L_{80}> <CAPA OID> 83 01 03 84 <L_{84}>$ $<CAPA domain> 7F4C <L_{7F4C}> <CHAT>'$ <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. • CHAT contains an OID and DDO 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: $'10 86 00 00 <L_c> 7C 00 <L_e>'$ 3. Send the given General Authenticate APDU to the eIDAS token without data: $'10 86 00 00 <L_c> 7C 02 81 00 <L_e>'$ 4. Perform key agreement: $'10 86 00 00 <L_c> 7C <L_{7C}> 83 <L_{83}> 04$ $<x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>'$ 5. Perform explicit authentication: $'00 86 00 00 <<L_c> 7C <L_{7C}> 85 <L_{85}> <MAC(PuK.ICC.DH,$ $K.MAC)> <L_e>'$ 6. Perform explicit verification (VERIFY command) with Secure Messaging: $'00 20 00 03 <L_c> <PIN>'$
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. $7C <L_{7C}> 80 <L_{80}> <\text{encrypted nonce}>$ and SW '90 00' in plain 3. $7C 02 82 00$ and SW '90 00' in plain 4. $7C 02 84 00$ and SW '90 00' in plain 5. $7C <L_{7C}> 86 <L_{86}> <MAC(PuK.IFD.DH, K.MAC)> 87 <L_{87}> <\text{CAR on latest PuK.CVCA.xy.n}> 88 <L_{88}> <\text{CAR on second most recent PuK.CVCA.xy.n if available}>$ and SW '90 00' in plain 6. '90 00' within a valid SM response

3.18.3 Test case EAC2_ISO7816_X_3

Test – ID	EAC2_ISO7816_X_3
Purpose	Negative test: Perform CAPA with break in command chaining (second APDU)
Version	EAC2_1.3
Profile	CAPA
Preconditions	<p>1. None, card recently activated, Smart-eID must be personalized with user-specific PIN</p>
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>' </p> <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. <p>2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce without chaining: '00 86 00 00 <L_c> 7C 00 <L_e>' </p>
Expected results	<p>1. '90 00' in plain</p> <p>2. Checking error in plain</p>

3.18.4 Test case EAC2_ISO7816_X_4

Test – ID	EAC2_ISO7816_X_4
Purpose	Negative test: Perform CAPA with break in command chaining (third APDU)
Version	EAC2_1.3
Profile	CAPA
Preconditions	<p>1. None, card recently activated, Smart-eID must be personalized with user-specific PIN</p>
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>' </p> <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. <p>2. Send the given General Authenticate APDU to the eIDAS token to get the</p>

Test plan for eID-Cards with EAC 2.0

	<p>encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>'</p> <p>3. Send the given General Authenticate APDU to the eIDAS token without data and without chaining: '00 86 00 00 <L_c> 7C 02 81 00 <L_e>'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. Checking error in plain

3.18.5 Test case EAC2_ISO7816_X_5

Test – ID	EAC2_ISO7816_X_5
Purpose	Negative test: Perform CAPA with break in command chaining (fourth APDU)
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <PACE OID> 83 01 03 84 <L₈₄> <PACE domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement without chaining: '00 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. Checking error in plain

3.18.6 Test case EAC2_ISO7816_X_6

Test – ID	EAC2_ISO7816_X_6
-----------	------------------

Purpose	Negative test: Perform CAPA without break in command chaining in last command
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' Perform explicit authentication without chaining: '10 86 00 00 <L_c> 7C <L_{7C}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> '90 00' in plain 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 7C 02 82 00 and SW '90 00' in plain 7C 02 84 00 and SW '90 00' in plain '68 83' in plain

3.18.7 Test case EAC2_ISO7816_X_7

Test – ID	EAC2_ISO7816_X_7
Purpose	Negative test: Perform CAPA with invalid password type
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eIDAS token in plain and invalid password type: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 01 84 <L₈₄> <CAPA domain>'

	<ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. <ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: $'10\ 86\ 00\ 00\ <L_c>\ 7C\ 00\ <L_e>'$ 3. Send the given General Authenticate APDU to the eIDAS token without data: $'10\ 86\ 00\ 00\ <L_c>\ 7C\ 02\ 81\ 00\ <L_e>'$ 4. Perform key agreement: $'10\ 86\ 00\ 00\ <L_c>\ 7C\ <L_{7c}>\ 83\ <L_{83}>\ 04\ \ <x\ (PuK.IFD.DH)>\ \ <y\ (PuK.IFD.DH)>\ <L_e>'$ 5. Perform explicit authentication: $'00\ 86\ 00\ 00\ <L_c>\ 7C\ <L_{7c}>\ 85\ <L_{85}>\ <MAC\ (PuK.ICC.DH,\ K.MAC)>\ <L_e>'$
Expected results	<ol style="list-style-type: none"> 1. '90 00' or Checking error in plain. Steps 2 to 5 are skipped in case of Checking error 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. Checking error in plain

3.18.8 Test case EAC2_ISO7816_X_8

Test – ID	EAC2 ISO7816 X 8
Purpose	Negative test: Perform CAPA with invalid PACE-light OID
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain and invalid OID: $'00\ 22\ 81\ A4\ <L_c>\ 80\ <L_{80}>\ <CAPA\ OID>\ 83\ 01\ 03\ 84\ <L_{84}>\ <CAPA\ domain>'$ <ul style="list-style-type: none"> • CAPA OID is an invalid CAPA-light OID specified in ICS. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: $'10\ 86\ 00\ 00\ <L_c>\ 7C\ 00\ <L_e>'$

	<p>3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>'</p> <p>4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>'</p> <p>5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' or Checking error in plain. Steps 2 to 5 are skipped in case of Checking error 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. Checking error in plain

3.18.9 Test case EAC2_ISO7816_X_9

Test – ID	EAC2_ISO7816_X_9
Purpose	Negative test: Perform CAPA without password type (DO 83)
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain and without password type DO: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess.
Expected results	<ol style="list-style-type: none"> 1. Checking error in plain

3.18.10 Test case EAC2_ISO7816_X_10

Test – ID	EAC2_ISO7816_X_10
Purpose	Negative test: Perform CAPA without OID (DO 80)
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-

Test plan for eID-Cards with EAC 2.0

	specific PIN
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token in plain and without OID (DO 80):</p> <p>'00 22 81 A4 <L_c> 83 01 03 84 <L₈₄> <CAPA domain>'</p> <ul style="list-style-type: none"> The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess.
Expected results	1. Checking error in plain

3.18.11 Test case EAC2_ISO7816_X_11

Test – ID	EAC2_ISO7816_X_11
Purpose	Negative test: Perform CAPA with empty password type (DO 83)
Version	EAC2 1.3
Profile	CAPA
Preconditions	<p>1. None, card recently activated, Smart-eID must be personalized with user-specific PIN</p>
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token in plain and without password type DO:</p> <p>'00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 00 84 <L₈₄> <CAPA domain>'</p> <ul style="list-style-type: none"> CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess.
Expected results	1. Checking error in plain

3.18.12 Test case EAC2_ISO7816_X_12

Test – ID	EAC2_ISO7816_X_12
Purpose	Negative test: Perform CAPA with empty OID (DO 80)
Version	EAC2 1.3
Profile	CAPA
Preconditions	<p>1. None, card recently activated, Smart-eID must be personalized with user-specific PIN</p>
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token in plain and without OID (DO 80):</p> <p>'00 22 81 A4 <L_c> 80 00 83 01 03 84 <L₈₄> <CAPA domain>'</p>

	<ul style="list-style-type: none"> The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess.
Expected results	1. Checking error in plain

3.18.13 Test case EAC2_ISO7816_X_13

Test – ID	EAC2 ISO7816 X 13
Purpose	Negative test: Perform CAPA with locked PIN. PIN of Smart-eID cannot be unlocked by user. CAPA must fail in this case. Note: Re-personalization of Smart-eID is necessary after execution of this test case.
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> None, card recently activated, Smart-eID must be personalized with user-specific PIN, PIN MUST be locked
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eIDAS token in plain with a locked PIN: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>'
Expected results	<ol style="list-style-type: none"> '63 C0' in plain '69 83' or '63 C0' in plain

3.18.14 Test case EAC2_ISO7816_X_14

Test – ID	EAC2 ISO7816 X 14
Purpose	Positive test: Perform CAPA with two nonces in GA
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>'

Test plan for eID-Cards with EAC 2.0

	<ul style="list-style-type: none"> CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. <ol style="list-style-type: none"> Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce a second time: '10 86 00 00 <L_c> 7C 00 <L_e>' Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>' Perform explicit verification (VERIFY command) with Secure Messaging: '00 20 00 03 <L_c> <PIN>'
Expected results	<ol style="list-style-type: none"> '90 00' in plain 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain or Checking error in plain. Steps 4 to 7 are skipped in case of Checking error 7C 02 82 00 and SW '90 00' in plain 7C 02 84 00 and SW '90 00' in plain 7C <L_{7c}> 86 <L₈₆> <MAC(PuK.IFD.DH, K.MAC)> and SW '90 00' in plain '90 00' within a valid SM response

3.18.15 Test case EAC2_ISO7816_X_15

Test – ID	EAC2_ISO7816_X_15
Purpose	Negative test: Perform CAPA with not-empty DO 81 in step 3
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128)

	<p>128) fitting the implemented algorithm.</p> <ul style="list-style-type: none"> The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. <ol style="list-style-type: none"> Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 01 00 <L_e>'
Expected results	<ol style="list-style-type: none"> '90 00' in plain 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain Checking error in plain

3.18.16 Test case EAC2_ISO7816_X_16

Test – ID	EAC2 ISO7816 X_16
Purpose	Positive test: Perform CAPA with a public key which does not belong to the elliptic curve.
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' Perform key agreement with a key which does not belong to the elliptic curve: '10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x (PuK.IFD.DH)> <y (PuK.IFD.DH)> <L_e>'
Expected results	<ol style="list-style-type: none"> '90 00' in plain 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 7C 02 82 00 and SW '90 00' in plain Checking error in plain

3.18.17 Test case EAC2_ISO7816_X_17

Test – ID	EAC2_ISO7816_X_17
Purpose	Negative test: Perform CAPA with providing a (0,0) key.
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ul style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement with a (0,0) key. The public key has to be coded as '04 x y' where both x and y have a size according to the prime, but filled with '00': '10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x(0)> <y(0)> <L_e>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. Checking error in plain

3.18.18 Test case EAC2_ISO7816_X_18

Test – ID	EAC2_ISO7816_X_18
Purpose	Negative test: Perform CAPA with VERIFY command without Secure Messaging
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ul style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>'

	<ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. <ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>' 6. Perform explicit verification (VERIFY command) without Secure Messaging: '00 20 00 03 <L_c> <PIN>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. 7C <L_{7c}> 86 <L₈₆> <MAC(PuK.IFD.DH, K.MAC)> and SW '90 00' in plain 6. Checking error in plain

3.18.19 Test case EAC2_ISO7816_X_19

Test – ID	EAC2_ISO7816_X_19
Purpose	Negative test: Perform CAPA with invalid P2 in VERIFY command
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess.

Test plan for eID-Cards with EAC 2.0

	<ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>' 6. Perform explicit verification (VERIFY command) with Secure Messaging but invalid P2: '00 20 00 02 <L_c> <PIN>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. 7C <L_{7c}> 86 <L₈₆> <MAC(PuK.IFD.DH, K.MAC)> and SW '90 00' in plain 6. Checking error in plain

3.18.20 Test case EAC2_ISO7816_X_20

Test – ID	EAC2 ISO7816 X 20
Purpose	Negative test: Perform CAPA without the intermediate step of General Authenticate (no mapping)
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Perform key agreement:

	'10 86 00 00 <L _c > 7C <L _{7C} > 83 <L ₈₃ > 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L _e >'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. Checking error in plain

3.18.21 Test case EAC2_ISO7816_X_21

Test – ID	EAC2 ISO7816 X 21
Purpose	Negative test: Perform CAPA with CHAT but without OID
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain> 7F4C <L_{7F4C}> <CHAT>'<ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. • CHAT contains a valid DDO (DO '53') but not OID 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7C}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain or Checking error in plain. Steps 2 to 5 are skipped in case of Checking error 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain or Checking error in plain 3. 7C 02 82 00 and SW '90 00' in plain or Checking error in plain 4. 7C 02 84 00 and SW '90 00' in plain or Checking error in plain 5. Checking error in plain

3.18.22 Test case EAC2_ISO7816_X_22

Test – ID	EAC2 ISO7816 X 22
Purpose	Negative test: Perform CAPA with CHAT but without DDO
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ul style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain> 7F4C <L_{7F4C}> <CHAT>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. • CHAT contains a valid OID (DO ‘06’) but no DDO (DO ‘53’) 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7C}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> 1. ‘90 00’ in plain or Checking error in plain. Steps 2 to 5 are skipped in case of Checking error 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW ‘90 00’ in plain or Checking error in plain 3. 7C 02 82 00 and SW ‘90 00’ in plain or Checking error in plain 4. 7C 02 84 00 and SW ‘90 00’ in plain or Checking error in plain 5. Checking error in plain

3.18.23 Test case EAC2_ISO7816_X_23

Test – ID	EAC2 ISO7816 X 23
Purpose	Negative test: Perform CAPA with CHAT but invalid tag for CHAT
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ul style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-

	specific PIN
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain> 7F4D <L_{7F4D}> <CHAT>'</p> <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. • CHAT contains a valid OID (DO '06') and DDO (DO '53') <p>2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>'</p> <p>3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>'</p> <p>4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>'</p> <p>5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7C}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'</p>
Expected results	<p>1. '90 00' in plain or Checking error in plain. Steps 2 to 5 are skipped in case of Checking error</p> <p>2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain or Checking error in plain</p> <p>3. 7C 02 82 00 and SW '90 00' in plain or Checking error in plain</p> <p>4. 7C 02 84 00 and SW '90 00' in plain or Checking error in plain</p> <p>5. Checking error in plain</p>

3.18.24 Test case EAC2_ISO7816_X_24

Test – ID	EAC2_ISO7816_X_24
Purpose	Negative test: Perform CAPA with CHAT but with mismatch in terminal type and CHAT
Version	EAC2_1.3
Profile	CAPA
Preconditions	<p>1. None, card recently activated, Smart-eID must be personalized with user-specific PIN</p>
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain> 7F4C <L_{7F4D}> <CHAT>'</p> <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm.

	<ul style="list-style-type: none"> The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. CHAT contains a valid OID (DO '06') and DDO (DO '53') but the length of the value in bytes matches not the terminal type specified in the CHAT <ol style="list-style-type: none"> Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x (PuK.IFD.DH)> <y (PuK.IFD.DH)> <L_e>' Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC (PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> '90 00' in plain or Checking error in plain. Steps 2 to 5 are skipped in case of Checking error 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain or Checking error in plain 7C 02 82 00 and SW '90 00' in plain or Checking error in plain 7C 02 84 00 and SW '90 00' in plain or Checking error in plain Checking error in plain

3.18.25 Test case EAC2_ISO7816_X_25

Test – ID	EAC2 ISO7816 X 25
Purpose	Negative test: Perform CAPA with CHAT but terminal type is not valid for CA+PA
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain> 7F4C <L_{7F4D}> <CHAT>' <ul style="list-style-type: none"> CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for PACE. The domain parameters are stored in EF.CardAccess. CHAT contains a OID (DO '06') and DDO (DO '53') where the most

	<p>significant two bits for the role are set to '0'</p> <ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain or Checking error in plain. Steps 2 to 5 are skipped in case of Checking error 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain or Checking error in plain 3. 7C 02 82 00 and SW '90 00' in plain or Checking error in plain 4. 7C 02 84 00 and SW '90 00' in plain or Checking error in plain 5. Checking error in plain

3.18.26 Test case EAC2_ISO7816_X_26

Test – ID	EAC2 ISO7816_X_26
Purpose	Negative test: Perform CAPA with an invalid data object tag in command MSE: Set AT
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 81 <L₈₁> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04

Test plan for eID-Cards with EAC 2.0

	<p>$\langle x \text{ (PuK.IFD.DH)} \rangle \langle y \text{ (PuK.IFD.DH)} \rangle <L_e>$,</p> <p>5. Perform explicit authentication: $'00 86 00 00 <L_c> 7C <L_{7c}> 85 <L_{85}> \langle \text{MAC (PuK.ICC.DH, K.MAC)} \rangle <L_e>'$</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' or Checking error in plain. Steps 2 to 5 are skipped in case of Checking error 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain or Checking error in plain. Steps 3 to 5 are skipped in case of Checking error 3. 7C 02 82 00 and SW '90 00' in plain or Checking error in plain. Steps 4 to 5 are skipped in case of Checking error 4. 7C 02 84 00 and SW '90 00' in plain or Checking error in plain. Step 5 is skipped in case of Checking error 5. Checking error in plain

3.18.27 Test case EAC2_ISO7816_X_27

Test – ID	EAC2_ISO7816_X_27
Purpose	Negative test: Perform CAPA with an unspecified OID in command MSE: Set AT
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: $'00 22 81 A4 <L_c> 80 <L_{80}> \langle \text{CAPA OID} \rangle 83 01 03 84 <L_{84}> \langle \text{CAPA domain} \rangle'$ <ul style="list-style-type: none"> • $\langle \text{CAPA OID} \rangle : \{\text{id-PACE 5}\}$. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: $'10 86 00 00 <L_c> 7C 00 <L_e>'$ 3. Send the given General Authenticate APDU to the eIDAS token without data: $'10 86 00 00 <L_c> 7C 02 81 00 <L_e>'$ 4. Perform key agreement: $'10 86 00 00 <L_c> 7C <L_{7c}> 83 <L_{83}> 04 \langle x \text{ (PuK.IFD.DH)} \rangle \langle y \text{ (PuK.IFD.DH)} \rangle <L_e>'$ 5. Perform explicit authentication: $'00 86 00 00 <L_c> 7C <L_{7c}> 85 <L_{85}> \langle \text{MAC (PuK.ICC.DH, K.MAC)} \rangle <L_e>'$
Expected results	<ol style="list-style-type: none"> 1. '90 00' or Checking error in plain. Steps 2 to 5 are skipped in case of Checking error 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain or

	<p>Checking error in plain. Steps 3 to 5 are skipped in case of Checking error</p> <ol style="list-style-type: none"> 3. 7C 02 82 00 and SW '90 00' in plain or Checking error in plain. Steps 4 to 5 are skipped in case of Checking error 4. 7C 02 84 00 and SW '90 00' in plain or Checking error in plain. Step 5 is skipped in case of Checking error 5. Checking error in plain
--	--

3.18.28 Test case EAC2_ISO7816_X_28

Test – ID	EAC2_ISO7816_X_28
Purpose	Negative test: Perform CAPA with an additional tag ,06‘ in command MSE: Set AT
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: $'00 22 81 A4 <L_c> 80 <L_{80}> 06 <L_{PACE\ OID}> <CAPA\ OID> 83 01 03 84 <L_{84}> <CAPA\ domain>'$ <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: $'10 86 00 00 <L_c> 7C 00 <L_e>'$ 3. Send the given General Authenticate APDU to the eIDAS token without data: $'10 86 00 00 <L_c> 7C 02 81 00 <L_e>'$ 4. Perform key agreement: $'10 86 00 00 <L_c> 7C <L_{7C}> 83 <L_{83}> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>'$ 5. Perform explicit authentication: $'00 86 00 00 <L_c> 7C <L_{7C}> 85 <L_{85}> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'$
Expected results	<ol style="list-style-type: none"> 1. '90 00' or Checking error in plain. Steps 2 to 5 are skipped in case of Checking error 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain or Checking error in plain. Steps 3 to 5 are skipped in case of Checking error 3. 7C 02 82 00 and SW '90 00' in plain or Checking error in plain. Steps 4 to 5 are skipped in case of Checking error 4. 7C 02 84 00 and SW '90 00' in plain or Checking error in plain. Step 5 is skipped in case of Checking error 5. Checking error in plain

3.18.29 Test case EAC2_ISO7816_X_29

Test – ID	EAC2_ISO7816_X_29
Purpose	Negative test: Perform CAPA with an invalid PACE domain in command MSE: Set AT
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ul style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: <code>'00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>'</code> <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • Invalid CAPA domain parameter unknown for the eID. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: <code>'10 86 00 00 <L_c> 7C 00 <L_e>'</code> 3. Send the given General Authenticate APDU to the eIDAS token without data: <code>'10 86 00 00 <L_c> 7C 02 81 00 <L_e>'</code> 4. Perform key agreement: <code>'10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>'</code> 5. Perform explicit authentication: <code>'00 86 00 00 <L_c> 7C <L_{7C}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'</code>
Expected results	<ol style="list-style-type: none"> 1. '90 00' or Checking error in plain. Steps 2 to 5 are skipped in case of Checking error 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain or Checking error in plain. Step 5 is skipped in case of Checking error 5. Checking error in plain

3.18.30 Test case EAC2_ISO7816_X_30

Test – ID	EAC2_ISO7816_X_30
Purpose	Negative test: Perform CAPA with an invalid dynamic authentication data tag while getting nonce
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ul style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-

	specific PIN
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>'</p> <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. <p>2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 8C 00 <L_e>'</p> <p>3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>'</p> <p>4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>'</p> <p>5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7C}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'</p>
Expected results	<p>1. '90 00' in plain</p> <p>2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain or Checking error in plain without a nonce. Steps 3 to 5 are skipped in case of Checking error</p> <p>3. 7C 02 82 00 and SW '90 00' in plain</p> <p>4. 7C 02 84 00 and SW '90 00' in plain</p> <p>5. Checking error in plain</p>

3.18.31 Test case EAC2_ISO7816_X_31

Test – ID	EAC2_ISO7816_X_31
Purpose	Negative test: Perform CAPA without a dynamic authentication data tag while getting nonce
Version	EAC2_1.3
Profile	CAPA
Preconditions	<p>1. None, card recently activated, Smart-eID must be personalized with user-specific PIN</p>
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>'</p> <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain

	<p>parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess.</p> <ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain or Checking error in plain without a nonce. Steps 3 to 5 are skipped in case of Checking error 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. Checking error in plain

3.18.32 Test case EAC2_ISO7816_X_32

Test – ID	EAC2 ISO7816_X_32
Purpose	Negative test: Perform CAPA with an additional dynamic authentication data tag while getting nonce
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 81 01 01 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data:

	<p>'10 86 00 00 <L_c> 7C 02 81 00 <L_e>'</p> <p>4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>'</p> <p>5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain or Checking error in plain without a nonce. Steps 3 to 5 are skipped in case of Checking error 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. Checking error in plain

3.18.33 Test case EAC2_ISO7816_X_33

Test – ID	EAC2_ISO7816_X_33
Purpose	Negative test: Perform CAPA with invalid dynamic authentication data tag in intermediate step
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 82 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'

Test plan for eID-Cards with EAC 2.0

Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain or Checking error in plain. Steps 4 to 5 are skipped in case of Checking error 4. 7C 02 84 00 and SW '90 00' in plain 5. Checking error in plain
------------------	--

3.18.34 Test case EAC2_ISO7816_X_34

Test – ID	EAC2_ISO7816_X_34
Purpose	Negative test: Perform CAPA without data tag in intermediate step
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7C}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain or Checking error in plain. Steps 4 to 5 are skipped in case of Checking error 4. 7C 02 84 00 and SW '90 00' in plain 5. Checking error in plain

3.18.35 Test case EAC2_ISO7816_X_35

Test – ID	EAC2 ISO7816 X 35
Purpose	Negative test: Perform CAPA without tag while performing key agreement
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ul style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7C}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain or Checking error in plain. Step 5 is skipped in case of Checking error 5. Checking error in plain

3.18.36 Test case EAC2_ISO7816_X_36

Test – ID	EAC2 ISO7816 X 36
Purpose	Negative test: Perform CAPA with invalid tag while performing key agreement
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ul style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain:

Test plan for eID-Cards with EAC 2.0

	<p>'00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>'</p> <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. <ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 8C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain or Checking error in plain. Step 5 is skipped in case of Checking error 5. Checking error in plain

3.18.37 Test case EAC2_ISO7816_X_37

Test – ID	EAC2 ISO7816 X 37
Purpose	Negative test: Perform CAPA without tag while performing key agreement
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the

	<p>encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>'</p> <ol style="list-style-type: none"> 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain or Checking error in plain. Step 5 is skipped in case of Checking error 5. Checking error in plain

3.18.38 Test case EAC2_ISO7816_X_38

Test – ID	EAC2 ISO7816 X_38
Purpose	Negative test: Perform CAPA with invalid tag while performing key agreement
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH,

Test plan for eID-Cards with EAC 2.0

	K.MAC) > <L _e >'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain or Checking error in plain. Step 5 is skipped in case of Checking error 5. Checking error in plain

3.18.39 Test case EAC2_ISO7816_X_39

Test – ID	EAC2_ISO7816_X_39
Purpose	Negative test: Perform CAPA without ,04‘ for key while performing key agreement
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7C}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain or Checking error in plain. Step 5 is skipped in case of Checking error 5. Checking error in plain

3.18.40 Test case EAC2_ISO7816_X_40

Test – ID	EAC2 ISO7816 X 40
Purpose	Negative test: Perform CAPA with incomplete public key while performing key agreement (y is missing)
Version	EAC2_1.3
Profile	CAPA
Preconditions	1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. </p> <p>2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>'</p> <p>3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>'</p> <p>4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <L_e>'</p> <p>5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7C}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'</p>
Expected results	<p>1. '90 00' in plain</p> <p>2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain</p> <p>3. 7C 02 82 00 and SW '90 00' in plain</p> <p>4. 7C 02 84 00 and SW '90 00' in plain or Checking error in plain. Step 5 is skipped in case of Checking error</p> <p>5. Checking error in plain</p>

3.18.41 Test case EAC2_ISO7816_X_41

Test – ID	EAC2 ISO7816 X 41
Purpose	Negative test: Perform CAPA without tag while performing explicit authentication
Version	EAC2_1.3
Profile	CAPA
Preconditions	1. None, card recently activated, Smart-eID must be personalized with user-

Test plan for eID-Cards with EAC 2.0

	specific PIN
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>'<ul style="list-style-type: none"> CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x (PuK.IFD.DH)> <y (PuK.IFD.DH)> <L_e>' Perform explicit authentication: '00 86 00 00 <L_c> 85 <L₈₅> <MAC (PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> '90 00' in plain 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 7C 02 82 00 and SW '90 00' in plain 7C 02 84 00 and SW '90 00' in plain Checking error in plain

3.18.42 Test case EAC2_ISO7816_X_42

Test – ID	EAC2 ISO7816 X 42
Purpose	Negative test: Perform CAPA with invalid tag while performing explicit authentication
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>'<ul style="list-style-type: none"> CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess.

	<ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 8C <L_{8c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. Checking error in plain

3.18.43 Test case EAC2_ISO7816_X_43

Test – ID	EAC2 ISO7816 X_43
Purpose	Negative test: Perform CAPA without tag while performing explicit authentication
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> <MAC(PuK.ICC.DH, K.MAC)>'

Test plan for eID-Cards with EAC 2.0

	<L _e >'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. '63 00' or checking error in plain

3.18.44 Test case EAC2_ISO7816_X_44

Test – ID	EAC2 ISO7816 X 44
Purpose	Negative test: Perform CAPA with invalid tag while performing explicit authentication
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>'<ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7C}> 87 <L₈₇> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. '63 00' or checking error in plain

3.18.45 Test case EAC2_ISO7816_X_45

Test – ID	EAC2 ISO7816 X 45
Purpose	Negative test: Perform CAPA with incorrect MAC computation while performing explicit authentication
Version	EAC2_1.3
Profile	CAPA
Preconditions	1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. </p> <p>2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>'</p> <p>3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>'</p> <p>4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>'</p> <p>5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7C}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC + 1)> <L_e>'</p>
Expected results	<p>1. '90 00' in plain</p> <p>2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain</p> <p>3. 7C 02 82 00 and SW '90 00' in plain</p> <p>4. 7C 02 84 00 and SW '90 00' in plain</p> <p>5. Checking error in plain</p>

3.18.46 Test case EAC2_ISO7816_X_46

Test – ID	EAC2 ISO7816 X 46
Purpose	Positive test: Perform CAPA with borderline case for x- and y- coordinates (small x coordinate) while performing key agreement
Version	EAC2_1.3
Profile	CAPA
Preconditions	1. None, card recently activated, Smart-eID must be personalized with user-specific PIN

Test plan for eID-Cards with EAC 2.0

Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' <ul style="list-style-type: none"> - Use an ephemeral public key with an x-coordinate requiring at least one byte less than the length of P. Pad with leading zero bytes. Generate key pairs at random until a public key satisfying the constraint is obtained 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>' 6. Perform explicit verification (VERIFY command) with Secure Messaging: '00 20 00 03 <L_c> <PIN>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. 7C <L_{7c}> 86 <L₈₆> <MAC(PuK.IFD.DH, K.MAC)> and SW '90 00' in plain 6. '90 00' within a valid SM response

3.18.47 Test case EAC2_ISO7816_X_47

Test – ID	EAC2_ISO7816_X_47
Purpose	Positive test: Perform CAPA with borderline case for x- and y- coordinates (large x coordinate) while performing key agreement
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄>

	<p><CAPA domain>`</p> <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. <ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: `10 86 00 00 <L_c> 7C 00 <L_e>` 3. Send the given General Authenticate APDU to the eIDAS token without data: `10 86 00 00 <L_c> 7C 02 81 00 <L_e>` 4. Perform key agreement: `10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>` - Use an ephemeral public key with an x-coordinate having its highest bit set to 1 5. Perform explicit authentication: `00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>` 6. Perform explicit verification (VERIFY command) with Secure Messaging: `00 20 00 03 <L_c> <PIN>`
Expected results	<ol style="list-style-type: none"> 1. ‘90 00’ in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW ‘90 00’ in plain 3. 7C 02 82 00 and SW ‘90 00’ in plain 4. 7C 02 84 00 and SW ‘90 00’ in plain 5. 7C <L_{7c}> 86 <L₈₆> <MAC(PuK.IFD.DH, K.MAC)> and SW ‘90 00’ in plain 6. ‘90 00’ within a valid SM response

3.18.48 Test case EAC2_ISO7816_X_48

Test – ID	EAC2_ISO7816_X_48
Purpose	Positive test: Perform CAPA with borderline case for x- and y- coordinates (small y coordinate) while performing key agreement
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: `00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>` • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128)

	<p>128) fitting the implemented algorithm.</p> <ul style="list-style-type: none"> The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. <ol style="list-style-type: none"> Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: $'10\ 86\ 00\ 00\ <L_c>\ 7C\ 00\ <L_e>'$ Send the given General Authenticate APDU to the eIDAS token without data: $'10\ 86\ 00\ 00\ <L_c>\ 7C\ 02\ 81\ 00\ <L_e>'$ Perform key agreement: $'10\ 86\ 00\ 00\ <L_c>\ 7C\ <L_{7c}>\ 83\ <L_{83}>\ 04\ \ <x\ (PuK.IFD.DH)>\ \ <y\ (PuK.IFD.DH)>\ <L_e>'$ - Use an ephemeral public key with a y-coordinate requiring at least one byte less than the length of P. Pad with leading zero bytes. Generate key pairs at random until a public key satisfying the constraint is obtained Perform explicit authentication: $'00\ 86\ 00\ 00\ <L_c>\ 7C\ <L_{7c}>\ 85\ <L_{85}>\ <MAC\ (PuK.ICC.DH,\ K.MAC)>\ <L_e>'$ Perform explicit verification (VERIFY command) with Secure Messaging: $'00\ 20\ 00\ 03\ <L_c>\ <PIN>'$
Expected results	<ol style="list-style-type: none"> '90 00' in plain 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 7C 02 82 00 and SW '90 00' in plain 7C 02 84 00 and SW '90 00' in plain 7C <L_{7c}> 86 <L₈₆> <MAC (PuK.IFD.DH, K.MAC)> and SW '90 00' in plain '90 00' within a valid SM response

3.18.49 Test case EAC2_ISO7816_X_49

Test – ID	EAC2_ISO7816_X_49
Purpose	Positive test: Perform CAPA with borderline case for x- and y- coordinates (large y coordinate) while performing key agreement
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eIDAS token in plain: $'00\ 22\ 81\ A4\ <L_c>\ 80\ <L_{80}>\ <CAPA\ OID>\ 83\ 01\ 03\ 84\ <L_{84}>\ <CAPA\ domain>'$ <ul style="list-style-type: none"> CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. The CAPA domain parameter reference is REQUIRED if the domain

	<p>parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess.</p> <ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' - Use an ephemeral public key with an y-coordinate having its highest bit set to 1 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>' 6. Perform explicit verification (VERIFY command) with Secure Messaging: '00 20 00 03 <L_c> <PIN>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. 7C <L_{7c}> 86 <L₈₆> <MAC(PuK.IFD.DH, K.MAC)> and SW '90 00' in plain 6. '90 00' within a valid SM response

3.18.50 Test case EAC2_ISO7816_X_50

Test – ID	EAC2_ISO7816_X_50
Version	Deleted in version 1.3.1

3.18.51 Test case EAC2_ISO7816_X_51

Test – ID	EAC2_ISO7816_X_51
Purpose	Negative test: Perform CAPA with a command interrupting the chain (after second command)
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>'

	<ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. <ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the READ BINARY command: '00 B0 9C 00 01' 4. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 5. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 6. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. '6883' in plain 4. Checking Error in plain 5. Checking Error in plain 6. Checking Error in plain

3.18.52 Test case EAC2_ISO7816_X_52

Test – ID	EAC2 ISO7816 X 52
Purpose	Negative test: Perform CAPA with a command interrupting the chain (after third command)
Version	EAC2 1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess.

	<ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Send the READ BINARY command: '00 B0 9C 00 01' 5. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 6. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>'
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. '6883' in plain 5. Checking Error in plain 6. Checking Error in plain

3.18.53 Test case EAC2 ISO7816_X_53

Test – ID	EAC2 ISO7816_X_53
Purpose	Negative test: Perform CAPA with a command interrupting the chain (after fourth command)
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement:

Test plan for eID-Cards with EAC 2.0

	<pre>'10 86 00 00 <Lc> 7C <L7c> 83 <L83> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <Le>'</pre> <p>5. Send the READ BINARY command: '00 B0 9C 00 01'</p> <p>6. Perform explicit authentication: '00 86 00 00 <Lc> 7C <L7c> 85 <L85> <MAC(PuK.ICC.DH, K.MAC)> <Le>'</p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L7c> 80 <L80> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. '6883' in plain 6. Checking Error in plain

3.18.54 Test case EAC2_ISO7816_X_54

Test – ID	EAC2_ISO7816_X_54
Purpose	Negative test: Perform CAPA with incomplete public key while performing key agreement (x is missing)
Version	EAC2_1.3
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. None, card recently activated, Smart-eID must be personalized with user-specific PIN
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <Lc> 80 <L80> <CAPA OID> 83 01 03 84 <L84> <CAPA domain>'<ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The PACE domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <Lc> 7C 00 <Le>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <Lc> 7C 02 81 00 <Le>' 4. Perform key agreement: '10 86 00 00 <Lc> 7C <L7c> 83 <L83> 04 <y(PuK.IFD.DH)> <Le>' 5. Perform explicit authentication: '00 86 00 00 <Lc> 7C <L7c> 85 <L85> <MAC(PuK.ICC.DH, K.MAC)> <Le>'

Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain or Checking error in plain. Step 5 is skipped in case of Checking error 5. Checking error in plain
------------------	---

3.18.55 Test case EAC2_ISO7816_X_55

Test – ID	EAC2 ISO7816_X_55
Purpose	Positive test case to reduce initial PIN retry counter by 1
Version	Smart-eID
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 2. The PIN MUST NOT have been blocked, deactivated or suspended 3. PIN retry counter MUST be set to initial value 4. Use INVALID PIN for VERIFY
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7C}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>' 6. Perform explicit verification (VERIFY command) with Secure Messaging: '00 20 00 03 <L_c> <PIN>' 7. Power off the chip and reinitialize connection 8. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm.

	<p>128) fitting the implemented algorithm.</p> <ul style="list-style-type: none"> The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess.
Expected results	<ol style="list-style-type: none"> '90 00' in plain 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 7C 02 82 00 and SW '90 00' in plain 7C 02 84 00 and SW '90 00' in plain 7C <L_{7C}> 86 <L₈₆> <MAC (PuK.IFD.DH, K.MAC)> and SW '90 00' in plain '63 00' or '63 CX' where X indicates the number of remaining verification tries, i.e. initial value – 1 (see ICS). True '63 CX' where X indicates the number of remaining verification tries, i.e. initial value – 1 (see ICS).

3.18.56 Test case EAC2_ISO7816_X_56

Test – ID	EAC2_ISO7816_X_56
Purpose	Positive test case to reset PIN retry counter to initial value
Version	Smart-eID
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> The PIN MUST NOT have been blocked, deactivated or suspended This test case MUST be performed immediately after Test case EAC2_ISO7816_X_55. Use VALID PIN for VERIFY
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7C}> 83 <L₈₃> 04 <x (PuK.IFD.DH)> <y (PuK.IFD.DH)> <L_e>'

	<p>5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC (PuK.ICC.DH, K.MAC)> <L_e>'</p> <p>6. Perform explicit verification (VERIFY command) with Secure Messaging: '00 20 00 03 <L_c> <PIN>'</p> <p>7. Power off the chip and reinitialize connection</p> <p>8. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. </p>
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. 7C <L_{7c}> 86 <L₈₆> <MAC (PuK.IFD.DH, K.MAC)> and SW '90 00' in plain 6. '90 00' within a valid SM response 7. True 8. '90 00'

3.18.57 Test case EAC2_ISO7816_X_57

Test – ID	EAC2_ISO7816_X_57
Purpose	Positive test case to change PIN
Version	Smart-eID
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked, deactivated or suspended 2. Use VALID PIN for VERIFY
Test scenario	<p>1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. </p> <p>2. Send the given General Authenticate APDU to the eIDAS token to get the</p>

Test plan for eID-Cards with EAC 2.0

	<p>encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>'</p> <ol style="list-style-type: none"> 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>' 6. Perform explicit verification (VERIFY command) with Secure Messaging: '00 20 00 03 <L_c> <PIN>' 7. Send the given Reset Retry Counter APDU to the eID Card. '0C 2C 02 03 <L_c> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '<new PIN>' 8. Power off the chip and reinitialize connection 9. Perform CAPA to verify new PIN, e.g. using Test case EAC2_ISO7816_X_1
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. 7C <L_{7c}> 86 <L₈₆> <MAC(PuK.IFD.DH, K.MAC)> and SW '90 00' in plain 6. '90 00' within a valid SM response 7. '90 00' within a valid SM response 8. True 9. True

3.18.58 Test case EAC2_ISO7816_X_58

Test – ID	EAC2_ISO7816_X_58
Purpose	Positive test case where PIN Authentication attempt with blocked PIN
Version	Smart-eID
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been deactivated 2. The PIN MUST have been blocked (e.g. using Test case EAC2_ISO7816_X_61)
Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>'<ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-)

	<p>128) fitting the implemented algorithm.</p> <ul style="list-style-type: none"> The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess.
Expected results	1. '63 C0' in plain

3.18.59 Test case EAC2_ISO7816_X_59

Test – ID	EAC2 ISO7816 X 59
Purpose	Negative test case to change PIN via authenticated PIN management
Version	Smart-eID
Profile	(CAPA, TA2 AT, CA2, NOT CNG PIN AR)
Preconditions	<ol style="list-style-type: none"> The CAPA mechanism MUST have been performed using PIN, PIN management must be allowed by CHAT The Terminal Authentication mechanism MUST have been performed (DV_CERT_17, AT_CERT_17b) The Chip Authentication MUST have been performed All APDUs are sent as valid Secure Messaging APDUs
Test scenario	<ol style="list-style-type: none"> Send the given Reset Retry Counter APDU to the eID Card. '0C 2C 02 03 <Lc> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> <Le>' <ul style="list-style-type: none"> <Cryptogram> contains the following encrypted data objects: '<new PIN>'
Expected results	1. '69 82' within a valid SM response

3.18.60 Test case EAC2_ISO7816_X_60

Test – ID	EAC2 ISO7816 X 60
Purpose	Positive test case to try to change PIN, but NEW PIN is too short
Version	Smart-eID
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> The PIN MUST NOT have been blocked, deactivated or suspended Use VALID PIN for VERIFY
Test scenario	<ol style="list-style-type: none"> Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>' <ul style="list-style-type: none"> CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters

Test plan for eID-Cards with EAC 2.0

	<p>are available for CAPA. The domain parameters are stored in EF.CardAccess.</p> <ol style="list-style-type: none"> 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>' 6. Perform explicit verification (VERIFY command) with Secure Messaging: '00 20 00 03 <L_c> <PIN>' 7. Send the given Reset Retry Counter APDU to the eID Card. '0C 2C 02 03 <L_c> 87 <L₈₇> 01 <Cryptogram> 8E 08 <Checksum> 00' <ul style="list-style-type: none"> • <Cryptogram> contains the following encrypted data objects: '<new PIN>' • NEW PIN MUST be shorter than minimum PIN length stated in ICS 8. Power off the chip and reinitialize connection 9. Perform CAPA to verify OLD PIN is still valid, e.g. using Test case EAC2_ISO7816_X_1
Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7c}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. 7C <L_{7c}> 86 <L₈₆> <MAC(PuK.IFD.DH, K.MAC)> and SW '90 00' in plain 6. '63 00' or '63 CX' where X indicates the number of remaining verification tries, i.e. initial value – 1 (see ICS). 7. '69 82' or other error within a valid SM response 8. True 9. True

3.18.61 Test case EAC2_ISO7816_X_61

Test – ID	EAC2_ISO7816_X_61
Purpose	Positive test case with blocked PIN
Version	Smart-eID
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> 1. The PIN MUST NOT have been blocked, deactivated or suspended 2. Use INVALID PIN for VERIFY

Test scenario	<ol style="list-style-type: none"> 1. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>'<ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 2. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 3. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 4. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 5. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>' 6. Perform explicit verification (VERIFY command) with Secure Messaging: '00 20 00 03 <L_c> <PIN>' 7. Power off the chip and reinitialize connection 8. Go to step 1 and repeat all steps until step 1 returns '63 C0' 9. Send the given MSE: Set AT APDU to the eIDAS token in plain: '00 22 81 A4 <L_c> 80 <L₈₀> <CAPA OID> 83 01 03 84 <L₈₄> <CAPA domain>'<ul style="list-style-type: none"> • CAPA OID is a valid CAPA OID (e.g. id-CAPA-AES-CBC-CMAC-128) fitting the implemented algorithm. • The CAPA domain parameter reference is REQUIRED if the domain parameters are ambiguous, i.e. more than one set of domain parameters are available for CAPA. The domain parameters are stored in EF.CardAccess. 10. Send the given General Authenticate APDU to the eIDAS token to get the encrypted nonce: '10 86 00 00 <L_c> 7C 00 <L_e>' 11. Send the given General Authenticate APDU to the eIDAS token without data: '10 86 00 00 <L_c> 7C 02 81 00 <L_e>' 12. Perform key agreement: '10 86 00 00 <L_c> 7C <L_{7c}> 83 <L₈₃> 04 <x(PuK.IFD.DH)> <y(PuK.IFD.DH)> <L_e>' 13. Perform explicit authentication: '00 86 00 00 <L_c> 7C <L_{7c}> 85 <L₈₅> <MAC(PuK.ICC.DH, K.MAC)> <L_e>' 14. Perform explicit verification (VERIFY command) with Secure Messaging: '00 20 00 03 <L_c> <PIN>'
---------------	---

Expected results	<ol style="list-style-type: none"> 1. '90 00' in plain 2. 7C <L_{7C}> 80 <L₈₀> <encrypted nonce> and SW '90 00' in plain 3. 7C 02 82 00 and SW '90 00' in plain 4. 7C 02 84 00 and SW '90 00' in plain 5. 7C <L_{7C}> 86 <L₈₆> <MAC (PuK.IFD.DH, K.MAC)> and SW '90 00' in plain 6. '63 00' or '63 CX' where X indicates the number of remaining verification tries, i.e. initial value – 1 (see ICS). 7. True 8. '63 CX'. Repeat until X=0. The Smart-eID MUST reduce X by 1 on each run. 9. '63 C0' 10. '90 00' or '69 83' or '69 82' or '63C0'. In case of an error or warning ('63C0') the following steps can be skipped. 11. '90 00' or '69 83' or '69 82' 12. '90 00' or '69 83' or '69 82' 13. '69 83' or '69 82' 14. '63 00' or '63 CX' where X indicates the number of remaining verification tries, i.e. initial value – 1 (see ICS).
------------------	--

4 Tests for layer 7 (Data Structure)

4.1 Unit EAC2_DATA_A, EF.CardAccess

This unit covers all tests about the coding of the elementary file EF.CardAccess containing relevant data for establishing the security protocols PACE, CA and TA.

4.1.1 Test case EAC2_DATA_A_1a

Test - ID	EAC2_DATA_A_1a
Purpose	Test the ASN.1 encoding of the SecurityInfos (PACE)
Version	EAC2 1.03
Profile	PACE, (TA2_AT or TA2_IS), (CA2 or CA3)
Preconditions	<ol style="list-style-type: none"> 1. EF.CardAccess MUST have been read from the eID Card
Test scenario	<ol style="list-style-type: none"> 1. The content of the SecurityInfos object MUST be encoded according to the SecurityInfos syntax definition. 2. At least one PACEInfo object MUST exist 3. For each supported set of proprietary PACE domain parameters a PACEDomainParameterInfo object MUST exist 4. At least one TerminalAuthenticationInfo MUST exist 5. Exactly one MobileEIDTypeInfo MUST exist in case of SMARTeID 6. At least one CAPAInfo MUST exist in case of CAPA 7. At least one CAPADomainParameterInfo MUST exist in case of CAPA

Expected results	<ol style="list-style-type: none"> 1. true 2. true 3. true 4. true 5. true 6. true 7. true
------------------	---

4.1.2 Test case EAC2_DATA_A_1b

Test - ID	EAC2_DATA_A_1b
Purpose	Test the ASN.1 encoding of the SecurityInfos (CA)
Version	EAC2_1.03
Profile	PACE, (TA2_AT or TA2_IS), (CA2 or CA3), CSTA
Preconditions	<ol style="list-style-type: none"> 1. EF.CardAccess MUST have been read from the eID Card
Test scenario	<ol style="list-style-type: none"> 1. The content of the SecurityInfos object MUST be encoded according to the SecurityInfos syntax definition. 2. At least one ChipAuthenticationInfo object MUST exist 3. At least one ChipAuthenticationDomainParameterInfo MUST exist
Expected results	<ol style="list-style-type: none"> 1. true 2. true 3. true

4.1.3 Test case EAC2_DATA_A_2

Test - ID	EAC2_DATA_A_2
Purpose	Test the ASN.1 encoding of the PACEInfo
Version	EAC2_1.03
Profile	PACE
Preconditions	<ol style="list-style-type: none"> 1. Test case EAC2_DATA_A_1 MUST have been performed 2. The data object containing SecurityInfos is parsed and this test is repeated for each PACEInfo element containing the OID specified in the EAC 2.0 specification [R8] and the version element set to 2.
Test scenario	<ol style="list-style-type: none"> 1. The PACEInfo element must follow the ASN.1 syntax definition in the EAC specification [R8]. 2. If standardized domain parameters are used the parameterID MUST reference a valid standardized domain parameter. If multiple proprietary domain parameters are used the parameterId reference in the PACEInfo MUST be coherent with the ICS (See A) and there MUST be a corresponding PACEDomainParameterInfo with compatible protocol OID (e.g. both contain DH-GM)
Expected results	<ol style="list-style-type: none"> 1. true 2. true

4.1.4 Test case EAC2_DATA_A_3

Test - ID	EAC2_DATA_A_3
Purpose	<p>Test the ASN.1 encoding of the PACEDomainParameterInfo</p> <p>This test case MUST be performed if proprietary domain parameters are used. If standardized domain parameters are used this test case MUST NOT be performed.</p>
Version	EAC2_1.03
Profile	PACE
Preconditions	<ol style="list-style-type: none"> 1. Test case EAC2_DATA_A_1 MUST have been performed 2. The data object containing SecurityInfos is parsed and this test is repeated for each PACEDomainParameterInfo element containing the OID specified in the EAC 2.0 specification [R8].
Test scenario	<ol style="list-style-type: none"> 1. The PACEDomainParameterInfo element must follow the ASN.1 syntax definition in the EAC specification [R8]. 2. The presence of the parameterId reference in the PACEDomainParameterInfo MUST be coherent with the ICS (See A) and there MUST be a corresponding PACEInfo with compatible protocol OID (e.g. both contain DH-GM) 3. If proprietary domain parameters are used the algorithm identifier domainParameter MUST be suitable to the key agreement protocol and its algorithm OID MUST be one of the following: <ul style="list-style-type: none"> • dhppublicnumber (OID: 1.2.840.10046.2.1) • id-ecPublicKey (OID: 1.2.840.10045.2.1) 4. The algorithm identifier's parameters MUST follow X9.42 (DH) [R11] or ECC specification (ECDH) [R6] and MUST be valid.
Expected results	<ol style="list-style-type: none"> 1. true 2. true 3. true 4. true

4.1.5 Test case EAC2_DATA_A_4

Test - ID	EAC2_DATA_A_4
Purpose	Test the ASN.1 encoding of the ChipAuthenticationInfo
Version	EAC2_1.0
Profile	CA2 or CA3
Preconditions	<ol style="list-style-type: none"> 1. Test case EAC2_DATA_A_1 MUST have been performed 2. The data object containing SecurityInfos is parsed and this test is repeated for each ChipAuthenticationInfo element containing the OID specified in the EAC specification [R8] and the version element set to 2. If there is no ChipAuthenticationInfo element available in EF.CardAccess, this test case can be skipped.
Test scenario	<ol style="list-style-type: none"> 1. The ChipAuthenticationInfo element must follow the ASN.1 syntax definition in the EAC specification [R8]. 2. The presence of the keyId reference in the ChipAuthenticationInfo MUST be coherent with the ICS (See A)

Expected results	<ol style="list-style-type: none"> 1. true 2. true
------------------	--

4.1.6 Test case EAC2_DATA_A_5

Test - ID	EAC2_DATA_A_5
Purpose	Test the ASN.1 encoding of the ChipAuthenticationDomainParameterInfo
Version	EAC2 1.03
Profile	CA2 or CA3
Preconditions	<ol style="list-style-type: none"> 1. Test case EAC2_DATA_A_1 MUST have been performed 2. The data object containing SecurityInfos is parsed and this test is repeated for each ChipAuthenticationDomainParameterInfo element containing the OID specified in the EAC 2.0 specification [R8]. If there is no ChipAuthenticationDomainParameterInfo element available in EF.CardAccess, this test case can be skipped.
Test scenario	<ol style="list-style-type: none"> 1. The ChipAuthenticationDomainParameterInfo element must follow the ASN.1 syntax definition in the EAC specification [R8]. 2. The presence of the keyId reference in the ChipAuthenticationDomainParameterInfo MUST be coherent with the ICS (See A) and there MUST be a corresponding ChipAuthenticationInfo with compatible protocol OID (e.g. both contain DH) 3. The algorithm identifier domainParamter MUST contain as parameters a valid Integer as specified in [R8] if standardized domain parameters are used. If proprietary domain parameters are used the algorithm identifier domainParameter MUST be suitable to the key agreement protocol and its algorithm OID MUST be one of the following: <ul style="list-style-type: none"> • dhpublicnumber (OID: 1.2.840.10046.2.1) • id-ecPublicKey (OID: 1.2.840.10045.2.1) 4. The algorithm identifier's parameters MUST follow X9.42 (DH) [R11] or ECC specification (ECDH) [R6] and MUST be valid.
Expected results	<ol style="list-style-type: none"> 1. true 2. true 3. true 4. true

4.1.7 Test case EAC2_DATA_A_6

Test - ID	EAC2_DATA_A_6
Purpose	Test the ASN.1 encoding of the TerminalAuthenticationInfo
Version	EAC2 1.0
Profile	TA2_AT or TA_IS
Preconditions	<ol style="list-style-type: none"> 1. Test case EAC2_DATA_A_1 MUST have been performed 2. The data object containing SecurityInfos is parsed and this test is repeated for each TerminalAuthenticationInfo element containing the OID specified in the EAC 2.0 specification [R8] and the version element set to 2.

Test plan for eID-Cards with EAC 2.0

Test scenario	1. The TerminalAuthenticationInfo element must follow the ASN.1 syntax definition in the EAC specification [R8].
Expected results	1. true

4.1.8 Test case EAC2_DATA_A_7

Test - ID	EAC2_DATA_A_7
Purpose	Test the ASN.1 encoding of the CardInfo
Version	EAC2_1.0
Profile	CardInfo
Preconditions	<ul style="list-style-type: none"> 1. Test case EAC2_DATA_A_1 MUST have been performed 2. The data object containing SecurityInfos is parsed
Test scenario	<ul style="list-style-type: none"> 1. The CardInfo element must follow the ASN.1 syntax definition in the EAC specification [R8].
Expected results	1. true

4.1.9 Test case EAC2_DATA_A_8

Test - ID	EAC2_DATA_A_8
Purpose	Test the ASN.1 encoding of the PSAInfo
Version	EAC2_1.0
Profile	PSAInfo
Preconditions	<ul style="list-style-type: none"> 1. Test case EAC2_DATA_A_1 MUST have been performed 2. The data object containing SecurityInfos is parsed
Test scenario	<ul style="list-style-type: none"> 1. The PSAInfo element must follow the ASN.1 syntax definition in the EAC specification [R8].
Expected results	1. true

4.1.10 Test case EAC2_DATA_A_9

Test - ID	EAC2_DATA_A_9
Purpose	Test the ASN.1 encoding of the PrivilegedTerminalInfo
Version	EAC2_1.0
Profile	PrivTerInfo
Preconditions	<ul style="list-style-type: none"> 1. Test case EAC2_DATA_A_1 MUST have been performed 2. The data object containing SecurityInfos is parsed
Test scenario	<ul style="list-style-type: none"> 1. The PrivilegedTerminalInfo element must follow the ASN.1 syntax definition in the EAC specification [R8].
Expected results	1. true

4.1.11 Test case EAC2_DATA_A_10

Test - ID	EAC2_DATA_A_10
-----------	----------------

Purpose	Test the ASN.1 encoding of the SecurityInfos (Smart-eID)
Version	Smart-eID
Profile	SMARTeID
Preconditions	<ol style="list-style-type: none"> EF.CardAccess MUST have been read from the eID Card
Test scenario	<ol style="list-style-type: none"> The content of the SecurityInfos object MUST be encoded according to the SecurityInfos syntax definition. Exactly one MobileEIDTypeInfo object MUST exist The type must be one of SECertified, SEEndorsed or HWKeyStore
Expected results	<ol style="list-style-type: none"> true true true

4.1.12 Test case EAC2_DATA_A_11

Test - ID	EAC2_DATA_A_11
Purpose	Test the ASN.1 encoding of the SecurityInfos (CAPAInfo)
Version	Smart-eID
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> EF.CardAccess MUST have been read from the eID Card
Test scenario	<ol style="list-style-type: none"> The content of the SecurityInfos object MUST be encoded according to the SecurityInfos syntax definition. At least one CAPAInfo object MUST exist Each CAPAInfo object MUST contain a valid protocol OID Each CAPAInfo object MUST contain a version number set to '2' If the eID uses standardized domain parameters or provides multiple explicit domain parameters for CA+PA, each CAPAInfo object MUST contain a valid parameterID to indicate the domain parameter identifier
Expected results	<ol style="list-style-type: none"> true true true true true

4.1.13 Test case EAC2_DATA_A_12

Test - ID	EAC2_DATA_A_12
Purpose	Test the ASN.1 encoding of the SecurityInfos (CAPADomainParameterInfo)
Version	Smart-eID
Profile	CAPA
Preconditions	<ol style="list-style-type: none"> EF.CardAccess MUST have been read from the eID Card
Test scenario	<ol style="list-style-type: none"> The content of the SecurityInfos object MUST be encoded according to the SecurityInfos syntax definition. At least one CAPADomainParameterInfo object MUST exist

	<ul style="list-style-type: none"> 3. Each CAPADomainParameterInfo object MUST contain a valid protocol OID 4. Each CAPADomainParameterInfo object MUST contain a valid domain parameter 5. If the eID provides multiple explicit domain parameters for CA+PA, each CAPADomainParameterInfo object MUST contain a valid parameterID to indicate the local domain parameter identifier
Expected results	<ul style="list-style-type: none"> 1. true 2. true 3. true 4. true 5. true

4.2 Unit EAC2_DATA_B, EF.CardSecurity

This unit covers all tests about the coding of the elementary file EF.CardSecurity containing the full set of data for establishing the security protocols PACE, CA and TA. This file is digitally signed.

4.2.1 Test case EAC2_DATA_B_1

Test - ID	EAC2_DATA_B_1
Purpose	Test the ASN.1 encoding of the SecurityInfos in EF.CardSecurity
Version	EAC2_1.03
Profile	PACE, (TA2_AT or TA2_IS), (CA2 or CA3)
Preconditions	<ul style="list-style-type: none"> 1. EF.CardSecurity MUST have been read from the eID Card
Test scenario	<ul style="list-style-type: none"> 1. The content of the SecurityInfos object MUST be encoded according to the SecurityInfos syntax definition. 2. EF.CardSecurity MUST be implemented as SignedData according to the EAC specification [R8]. 3. The signature MUST be verified. 4. At least one PACEInfo object MUST exist 5. For each supported set of proprietary PACE domain parameters a PACEDomainParameterInfo object MUST exist 6. At least one ChipAuthenticationInfo object MUST exist 7. At least one ChipAuthenticationDomainParameterInfo MUST exist 8. At least one ChipAuthenticationPublicKeyInfo MUST exist 9. At least one TerminalAuthenticationInfo MUST exist
Expected results	<ul style="list-style-type: none"> 1. true 2. true 3. true 4. true

	5. true 6. true 7. true 8. true 9. true
--	---

4.2.2 Test cases EAC2_DATA_B_2 to EAC2_DATA_B_7

Test cases EAC2_DATA_B_2 to EAC2_DATA_B_7 are equally performed on SecurityInfo objects from EF.CardSecurity like test cases EAC2_DATA_A_2 to EAC2_DATA_A_7 were performed on SecurityInfo objects EF.CardAccess before. References to EAC2_DATA_A_1 are replaced by references to EAC2_DATA_B_1. The profile CSTA is only relevant for test suite EAC2_DATA_A but not for test suite EAC2_DATA_B. Also the conditions of test cases EAC2_DATA_A_4 and EAC2_DATA_A_5 are only relevant for test suite EAC2_DATA_A but not for test suite EAC2_DATA_B.

4.2.3 Test case EAC2_DATA_B_8

Test - ID	EAC2_DATA_B_8
Purpose	Test the ASN.1 encoding of the ChipAuthenticationPublicKeyInfo
Version	EAC2 1.03
Profile	CA2 or CA3
Preconditions	1. Test case EAC2_DATA_B_1 MUST have been performed 2. The data object containing SecurityInfos is parsed and this test is repeated for each ChipAuthenticationPublicKeyInfo element containing the OID specified in the EAC 2.0 specification [R8].
Test scenario	1. The ChipAuthenticationPublicKeyInfo element must follow the ASN.1 syntax definition in the EAC specification [R8]. 2. The presence of the keyId reference in the ChipAuthenticationPublicKeyInfo MUST be coherent with the ICS (See Annex A) and there MUST be corresponding ChipAuthenticationInfo and ChipAuthenticationDomainParameterInfo with compatible protocol OID (e.g. all contain DH) 3. The algorithm identifier MUST contain as parameters a valid Integer as specified in [R8] if standardized domain parameters are used. If proprietary domain parameters are used the algorithm identifier MUST be suitable to the key agreement protocol and its algorithm OID MUST be one of the following: <ul style="list-style-type: none"> • dhpublicnumber (OID: 1.2.840.10046.2.1) • id-ecPublicKey (OID: 1.2.840.10045.2.1) 4. The algorithm identifier's parameters MUST follow X9.42 (DH) [R11] or ECC specification (ECDH) [R6] and MUST be valid.
Expected results	1. true 2. true 3. true

	4. true
--	---------

4.2.4 Test case EAC2_DATA_B_9

Test - ID	EAC2_DATA_B_9
Purpose	Test the ASN.1 encoding of the RestrictedIdentificationInfo
Version	EAC2 1.0
Profile	RI
Preconditions	<ol style="list-style-type: none"> 1. Test case EAC2_DATA_B_1 MUST have been performed and at least one RestrictedIdentificationInfo object MUST exist 2. The data object containing SecurityInfos is parsed and this test is repeated for each RestrictedIdentificationInfo element containing the OID specified in the EAC specification [R8] and the version element set to 1.
Test scenario	<ol style="list-style-type: none"> 1. The RestrictedIdentificationInfo element must follow the ASN.1 syntax definition in the EAC specification [R8]. 2. The presence of the keyId reference in the RestrictedIdentificationInfo MUST be coherent with the ICS (See Annex A)
Expected results	<ol style="list-style-type: none"> 1. true 2. true

4.2.5 Test case EAC2_DATA_B_10

Test - ID	EAC2_DATA_B_10
Purpose	Test the ASN.1 encoding of the RestrictedIdentificationDomainParameterInfo
Version	EAC2 1.03
Profile	RI_DP
Preconditions	<ol style="list-style-type: none"> 1. Test case EAC2_DATA_B_1 MUST have been performed and exactly one RestrictedIdentificationDomainParameterInfo object MUST exist 2. The data object containing SecurityInfos is parsed.
Test scenario	<ol style="list-style-type: none"> 1. The RestrictedIdentificationDomainParameterInfo element must follow the ASN.1 syntax definition in the EAC specification [R8]. 2. The algorithm identifier domainParamter MUST contain as parameters a valid Integer as specified in [R8] if standardized domain parameters are used. If proprietary domain parameters are used the algorithm identifier domainParameter MUST be suitable to the key agreement protocol and its algorithm OID MUST be one of the following: <ul style="list-style-type: none"> • dhpublicnumber (OID: 1.2.840.10046.2.1) • id-ecPublicKey (OID: 1.2.840.10045.2.1) 3. The algorithm identifier's parameters MUST follow X9.42 (DH) [R11] or ECC specification (ECDH) [R6] and MUST be valid.
Expected results	<ol style="list-style-type: none"> 1. true 2. true 3. true

4.2.6 Test case EAC2_DATA_B_11

Test - ID	EAC2_DATA_B_11
Purpose	Test the coherency between EF.CardSecurity and EF.CardAccess
Version	EAC2_1.1
Profile	PACE
Preconditions	<ol style="list-style-type: none"> 1. EF.CardAccess MUST have been read successfully 2. EF.CardSecurity MUST have been read successfully
Test scenario	<ol style="list-style-type: none"> 1. Check that the following SecurityInfo structures which are stored in EF.CardAccess are duplicated in EF.CardSecurity (PrivilegedTerminalInfos MUST be ignored): <ul style="list-style-type: none"> - PACEInfo - PACEDomainParameterInfo - ChipAuthenticationInfo - ChipAuthenticationDomainParameterInfo - PSAInfo (in case of PSAInfo) - TerminalAuthenticationInfo - PSMInfo (in case of PSMInfo) - CardInfo (in case of CardInfo) - MobileEIDTypeInfo (in case of SMARTeID) - CAPAInfo (in case of CAPA) - CAPADomainParameterInfo (in case of CAPA)
Expected results	<ol style="list-style-type: none"> 1. Each SecurityInfo structure of the list above is stored in the EF.CardAccess is also present in EF.CardSecurity

4.2.7 Test case EAC2_DATA_B_12

Test - ID	EAC2_DATA_B_12
Purpose	Test the ASN.1 encoding of the SecurityInfos (Smart-eID) and the coherency to EF.CardAccess
Version	Smart-eID
Profile	SMARTeID
Preconditions	<ol style="list-style-type: none"> 1. EF.CardAccess MUST have been read from the eID Card 1. EF.CardSecurity MUST have been read from the eID Card
Test scenario	<ol style="list-style-type: none"> 1. The content of the SecurityInfos object MUST be encoded according to the SecurityInfos syntax definition. 2. Exactly one MobileEIDTypeInfo object MUST exist 3. The type must be one of SECertified, SEEndorsed or HWKeyStore 4. Check that MobileEIDTypeInfo stored in EF.CardAccess is duplicated in EF.CardSecurity
Expected results	<ol style="list-style-type: none"> 1. true 2. true

	<ul style="list-style-type: none"> 3. true 4. true
--	--

4.2.8 Test case EAC2_DATA_B_13

Test - ID	EAC2_DATA_B_13
Purpose	Test the ASN.1 encoding of the SecurityInfos (CAPAInfo) and the coherency to EF.CardAccess
Version	Smart-eID
Profile	CAPA
Preconditions	<ul style="list-style-type: none"> 1. EF.CardAccess MUST have been read from the eID Card 1. EF.CardSecurity MUST have been read from the eID Card
Test scenario	<ul style="list-style-type: none"> 1. The content of the SecurityInfos object MUST be encoded according to the SecurityInfos syntax definition. 2. At least one CAPAInfo object MUST exist 3. The content of CAPAInfo MUST be in accordance to EAC2_DATA_A_11 4. Check that CAPAInfo stored in EF.CardAccess is duplicated in EF.CardSecurity
Expected results	<ul style="list-style-type: none"> 1. true 2. true 3. true 4. true

4.2.9 Test case EAC2_DATA_B_14

Test - ID	EAC2_DATA_B_14
Purpose	Test the ASN.1 encoding of the SecurityInfos (CAPADomainParameterInfo) and the coherency to EF.CardAccess
Version	Smart-eID
Profile	CAPA
Preconditions	<ul style="list-style-type: none"> 1. EF.CardAccess MUST have been read from the eID Card 1. EF.CardSecurity MUST have been read from the eID Card
Test scenario	<ul style="list-style-type: none"> 1. The content of the SecurityInfos object MUST be encoded according to the SecurityInfos syntax definition. 2. At least one CAPADomainParameterInfo object MUST exist 3. The content of CAPADomainParameterInfo MUST be in accordance to EAC2_DATA_A_11 4. Check that CAPADomainParameterInfo stored in EF.CardAccess is duplicated in EF.CardSecurity
Expected results	<ul style="list-style-type: none"> 1. true 2. true 3. true 4. true

4.3 Unit EAC2_EIDDATA_B eID Data Groups

This unit covers all tests about the coding of the elementary files of the eID application. Due to the simplicity of the encoded elements all data groups are tested within one test unit. Not all data groups must be present in all cases of implementation, therefore only the tests fitting the eID Card personalization must be performed.

4.3.1 Test case EAC2_EIDDATA_B_1

Test - ID	EAC2_EIDDATA_B_1
Purpose	Test the ASN.1 encoding of the eID DG1 elementary file
Version	EAC2 1.0
Profile	(SMARTeID or eID), DG1
Preconditions	1. DG1 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the DocumentType syntax definition.
Expected results	1. true

4.3.2 Test case EAC2_EIDDATA_B_2

Test - ID	EAC2_EIDDATA_B_2
Purpose	Test the ASN.1 encoding of the eID DG2 elementary file
Version	EAC2 1.0
Profile	(SMARTeID or eID), DG2
Preconditions	1. DG2 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the IssuingState syntax definition.
Expected results	1. true

4.3.3 Test case EAC2_EIDDATA_B_3

Test - ID	EAC2_EIDDATA_B_3
Purpose	Test the ASN.1 encoding of the eID DG3 elementary file
Version	EAC2 1.0
Profile	(SMARTeID or eID), DG3
Preconditions	1. DG3 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the DateOfExpiry syntax definition.
Expected results	1. true

4.3.4 Test case EAC2_EIDDATA_B_4

Test - ID	EAC2_EIDDATA_B_4
Purpose	Test the ASN.1 encoding of the eID DG4 elementary file
Version	EAC2_1.0
Profile	(SMARTeID or eID), DG4
Preconditions	1. DG4 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the GivenNames syntax definition.
Expected results	1. true

4.3.5 Test case EAC2_EIDDATA_B_5

Test - ID	EAC2_EIDDATA_B_5
Purpose	Test the ASN.1 encoding of the eID DG5 elementary file
Version	EAC2_1.0
Profile	(SMARTeID or eID), DG5
Preconditions	1. DG5 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the FamilyNames syntax definition.
Expected results	1. true

4.3.6 Test case EAC2_EIDDATA_B_6

Test - ID	EAC2_EIDDATA_B_6
Purpose	Test the ASN.1 encoding of the eID DG6 elementary file
Version	EAC2_1.0
Profile	(SMARTeID or eID), DG6
Preconditions	1. DG6 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the NomDePlume syntax definition.
Expected results	1. true

4.3.7 Test case EAC2_EIDDATA_B_7

Test - ID	EAC2_EIDDATA_B_7
Purpose	Test the ASN.1 encoding of the eID DG7 elementary file
Version	EAC2_1.0
Profile	(SMARTeID or eID), DG7
Preconditions	1. DG7 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the AcademicTitle syntax definition.
Expected results	1. true

4.3.8 Test case EAC2_EIDDATA_B_8

Test - ID	EAC2_EIDDATA_B_8
Purpose	Test the ASN.1 encoding of the eID DG8 elementary file
Version	EAC2_1.0
Profile	(SMARTeID or eID), DG8
Preconditions	1. DG8 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the DateOfBirth syntax definition.
Expected results	1. true

4.3.9 Test case EAC2_EIDDATA_B_9

Test - ID	EAC2_EIDDATA_B_9
Purpose	Test the ASN.1 encoding of the eID DG9 elementary file
Version	EAC2_1.0
Profile	(SMARTeID or eID), DG9
Preconditions	1. DG9 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the PlaceOfBirth syntax definition.
Expected results	1. true

4.3.10 Test case EAC2_EIDDATA_B_10

Test - ID	EAC2_EIDDATA_B_10
Purpose	Test the ASN.1 encoding of the eID DG10 elementary file
Version	EAC2_1.0
Profile	(SMARTeID or eID), DG10
Preconditions	1. DG10 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the Nationality syntax definition.
Expected results	1. true

4.3.11 Test case EAC2_EIDDATA_B_11

Test - ID	EAC2_EIDDATA_B_11
Purpose	Test the ASN.1 encoding of the eID DG11 elementary file
Version	EAC2_1.0
Profile	(SMARTeID or eID), DG11
Preconditions	1. DG11 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the Sex syntax definition.
Expected results	1. true

4.3.12 Test case EAC2_EIDDATA_B_12

Test - ID	EAC2_EIDDATA_B_12
Purpose	Test the ASN.1 encoding of the eID DG12 elementary file
Version	EAC2_1.0
Profile	(SMARTeID or eID), DG12
Preconditions	1. DG12 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the OptionalDataR syntax definition.
Expected results	1. true

4.3.13 Test case EAC2_EIDDATA_B_13

Test - ID	EAC2_EIDDATA_B_13
Purpose	Test the ASN.1 encoding of the eID DG17 elementary file
Version	EAC2_1.0
Profile	(SMARTeID or eID), DG17
Preconditions	1. DG17 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the PlaceOfResidence syntax definition.
Expected results	1. true

4.3.14 Test case EAC2_EIDDATA_B_14

Test - ID	EAC2_EIDDATA_B_14
Purpose	Test the ASN.1 encoding of the eID DG18 elementary file
Version	EAC2_1.0
Profile	(SMARTeID or eID), DG18
Preconditions	1. DG18 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the MunicipalityID syntax definition.
Expected results	1. true

4.3.15 Test case EAC2_EIDDATA_B_15

Test - ID	EAC2_EIDDATA_B_15
Purpose	Test the ASN.1 encoding of the eID DG19 elementary file
Version	EAC2_1.0
Profile	(SMARTeID or eID), DG19
Preconditions	1. DG19 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the ResidencePermitI syntax definition.
Expected results	1. true

4.3.16 Test case EAC2_EIDDATA_B_16

Test - ID	EAC2_EIDDATA_B_16
Purpose	Test the ASN.1 encoding of the eID DG20 elementary file
Version	EAC2_1.0
Profile	(SMARTeID or eID), DG20
Preconditions	1. DG20 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the ResidencePermitII syntax definition.
Expected results	1. true

4.3.17 Test case EAC2_EIDDATA_B_17

Test - ID	EAC2_EIDDATA_B_17
Purpose	Test the ASN.1 encoding of the eID DG21 elementary file
Version	EAC2_1.0
Profile	(SMARTeID or eID), DG21
Preconditions	1. DG21 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the PhoneNumber syntax definition.
Expected results	1. true

4.3.18 Test case EAC2_EIDDATA_B_18

Test - ID	EAC2_EIDDATA_B_18
Purpose	Test the ASN.1 encoding of the eID DG22 elementary file
Version	EAC2_1.1
Profile	(SMARTeID or eID), DG22
Preconditions	1. DG22 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the EMailAddress syntax definition.
Expected results	1. true

4.3.19 Test case EAC2_EIDDATA_B_19

Test - ID	EAC2_EIDDATA_B_19
Purpose	Test the ASN.1 encoding of the eID DG13 elementary file
Version	EAC2_1.1
Profile	(SMARTeID or eID), DG13
Preconditions	1. DG13 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the BirthName syntax definition.
Expected results	1. true

4.3.20 Test case EAC2_EIDDATA_B_20

Test - ID	EAC2_EIDDATA_B_20
Purpose	Test the ASN.1 encoding of the eID DG14 elementary file
Version	EAC2_1.1
Profile	(SMARTeID or eID), DG14
Preconditions	1. DG14 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the WrittenSignature syntax definition.
Expected results	1. true

4.3.21 Test case EAC2_EIDDATA_B_21

Test - ID	EAC2_EIDDATA_B_21
Purpose	Test the ASN.1 encoding of the eID DG15 elementary file
Version	EAC2_1.1
Profile	(SMARTeID or eID), DG15
Preconditions	1. DG15 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the Date syntax definition.
Expected results	1. true

4.3.22 Test case EAC2_EIDDATA_B_22

Test - ID	EAC2_EIDDATA_B_22
Purpose	Test the ASN.1 encoding of the eID DG1 elementary file
Version	EAC2_1.0
Profile	SMARTeID, DG1
Preconditions	1. DG1 MUST have been read from the eID Card
Test scenario	1. The content of the data object MUST be encoded according to the DocumentType syntax definition and the document type MUST be ‘OA’.
Expected results	1. true

4.4 Unit EAC2_DATA_C, EF.ChipSecurity

This unit covers all tests about the coding of the elementary file EF.ChipSecurity containing the signed SecurityInfos supported by the MRTD chip. This file SHALL be restricted to privileged terminals.

4.4.1 Test case EAC2_DATA_C_1

Test - ID	EAC2_DATA_C_1
Purpose	Test the ASN.1 encoding of the SecurityInfos in EF.ChipSecurity
Version	EAC2_1.1
Profile	CS
Preconditions	<ul style="list-style-type: none"> 1. EF.ChipSecurity MUST have been read from the eID Card
Test scenario	<ul style="list-style-type: none"> 1. The content of the SecurityInfos object MUST be encoded according to the SecurityInfos syntax definition. 2. EF.ChipSecurity MUST be implemented as SignedData according to the EAC specification [R8]. 3. The signature MUST be verified. 4. At least one PACEInfo object MUST exist 5. For each supported set of proprietary PACE domain parameters a PACEDomainParameterInfo object MUST exist 6. At least one ChipAuthenticationInfo object MUST exist 7. At least one ChipAuthenticationDomainParameterInfo MUST exist 8. At least one ChipAuthenticationPublicKeyInfo MUST exist 9. At least one TerminalAuthenticationInfo MUST exist 10. A CardInfoLocator MAY exist 11. A PrivilegedTerminalInfo MAY exist
Expected results	<ul style="list-style-type: none"> 1. true 2. true 3. true 4. true 5. true 6. true 7. true 8. true 9. true 10. true 11. true

4.4.2 Test cases EAC2_DATA_C_2 to EAC2_DATA_C_10

Test cases EAC2_DATA_C_2 to EAC2_DATA_C_7 are equally performed on SecurityInfo objects from EF.ChipSecurity like test cases EAC2_DATA_A_2 to EAC2_DATA_A_7 were performed on SecurityInfo objects in EF.CardAccess before. References to EAC2_DATA_A_1 are replaced by references to EAC2_DATA_C_1.

Test case EAC2_DATA_C_8 to EAC2_DATA_C10 are equally performed on SecurityInfo objects from EF.ChipSecurity like test cases EAC2_DATA_B_8 to EAC2_DATA_B10 were performed on SecurityInfo objects in EF.CardSecurity before. References to EAC2_DATA_B_1 are replaced by references to EAC2_DATA_C_1.

Test plan for eID-Cards with EAC 2.0

The profile CSTA is only relevant for test suite EAC2_DATA_A but not for test suite EAC2_DATA_C. Also the conditions of test cases EAC2_DATA_A_4 and EAC2_DATA_A_5 are only relevant for test suite EAC2_DATA_A but not for test suite EAC2_DATA_C.

4.4.3 Test case EAC2_DATA_C_11

Test - ID	EAC2 DATA C 11
Purpose	Test the ASN.1 encoding of the PrivilegedTerminalInfo
Version	EAC2 1.1
Profile	CS
Preconditions	<ol style="list-style-type: none">1. Test case EAC2_DATA_C_1 MUST have been performed and exactly one PrivilegedTerminalInfo object MUST exist2. The data object containing SecurityInfos is parsed.
Test scenario	<ol style="list-style-type: none">1. The eIDSecurityInfo element must follow the ASN.1 syntax definition in the EAC specification [R8].2. For each ChipAuthenticationInfo encapsulated in PrivilegedTerminalInfo, the corresponding ChipAuthenticationPublicKeyInfo MUST also be included in PrivilegedTerminalInfo.3. The presence of the keyId reference in the PrivilegedTerminalInfo MUST be coherent with the ICS (See Annex A)
Expected results	<ol style="list-style-type: none">1. true2. true3. true

4.4.4 Test case EAC2_DATA_C_12

Test - ID	EAC2 DATA C 12
Purpose	Test the ASN.1 encoding of the eIDSecurityInfo
Version	EAC2 1.1
Profile	CS
Preconditions	<ol style="list-style-type: none">1. Test case EAC2_DATA_C_1 MUST have been performed and exactly one eIDSecurityInfo object MUST exist2. The data object containing SecurityInfos is parsed.
Test scenario	<ol style="list-style-type: none">1. The eIDSecurityInfo element must follow the ASN.1 syntax definition in the EAC specification [R8].
Expected results	<ol style="list-style-type: none">1. true

Annex A Implementation conformance statement

In order to set up the tests properly, an applicant SHALL provide the information specified in this annex. Some tests defined in this document are depending on the supported functionality of the eID Card. The test results will only cover the function declared in this statement.

A.1 Supported profiles

Tests that require functions not supported by the provided eID Card will be skipped during the tests. Please specify the profiles supported by the provided sample. For details on the profiles, please refer to section 2.2.

Application Profile	Applicant declaration (YES or NO)
ePassport	
eID	
eSign	
Smart-eID	

Protocol Profile	Applicant declaration (YES or NO)
Migration of the cryptographic system	
Certificate date validation	
Restricted Identification	
Restricted Identification Domain Parameters	
Auxiliary Data Verification	
Change PIN after PACE using PUK allowed	
Change PIN for authentication terminals with “PIN Management” access rights allowed	
Change CAN for authentication terminals with “PIN Management” access rights allowed	
BAC	
PACE	
TA2_IS	
TA2_AT	
CA1	
CA2	
CA3	
CA3_ReUse	
Chip Security	
Envelope mechanism (ENV)	
Compare (CMP)	
AUTH_EXT	
CSTA (EF.CardSecurity is protected by TA)	
PSAInfo	

Protocol Profile	Applicant declaration (YES or NO)
PSMInfo	
CardInfo	
PrivTerInfo	
CAPA (aka PACE-light)	

Algorithm Profile	Applicant declaration (YES or NO)
For Terminal Authentication based on ECDSA algorithm, include domain parameter in link certificate (LINK_CERT_7, LINK_CERT_8, LINK_CERT_9)	

List of supported data groups:

DG	1	2	3	4	5	6	7	8	9	1	2	2	2							
	0	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	0
ePassport																		not available		
(Smart-)eID																				

List of data groups supporting the command COMPARE for (Smart-)eID:

Auxiliary data	Object Identifier	DG	Applicant declaration (YES or NO)
Age Verification	id-DateOfBirth OID	DG 8	
Document Validity Verification	id-DateOfExpiry OID	DG 3	
Municipality ID Verification	id-MunicipalityID OID	DG 18	
Data Group Content Verification	id-DGContent OID	DG 1	
		DG 2	
		DG 3	
		DG 4	
		DG 5	
		DG 6	
		DG 7	
		DG 8	
		DG 9	
		DG 10	
		DG 11	
		DG 12	
		DG 13	
		DG 14	
		DG 15	
		DG 16	
		DG 17	
		DG 18	

	DG 19	
	DG 20	
	DG 21	
	DG 22	

A.2 Supported cryptographic algorithm

The applicant of the passport under test SHALL declare the cryptosystem (signature algorithm and hash algorithm) used to perform the Terminal Authentication.

Signature algorithm	Key size (incl. curve name for ECDSA)	Hash algorithm

A.3 Cryptosystem migration policy

If the eID Card under test supports the migration to another cryptosystem, the applicant SHALL provide the list of supported target(s) cryptosystem(s) (signature algorithm and hash algorithm).

Note: For each target algorithm specified in this table, the test unit EAC2_ISO7816_N has to be performed. Afterward, the complete test set has to be repeated for each new algorithm.

Signature algorithm	Key size (incl. curve name for ECDSA)	Hash algorithm

A.4 EF.CardSecurity information

The applicant SHALL declare all supported protocol suites. The EF.CardSecurity file SHALL contain all necessary SecurityInfo objects. Algorithm profiles like DH/ECDH are directly derived from this table.

Protocol Suite	Applicant declaration (YES or NO)
id-PACE-DH-GM-3DES-CBC-CBC	
id-PACE-DH-GM-AES-CBC-CMAC-128	
id-PACE-DH-GM-AES-CBC-CMAC-192	
id-PACE-DH-GM-AES-CBC-CMAC-256	
id-PACE-ECDH-GM-3DES-CBC-CBC	
id-PACE-ECDH-GM-AES-CBC-CMAC-128	

Test plan for eID-Cards with EAC 2.0

Protocol Suite	Applicant declaration (YES or NO)
id-PACE-ECDH-GM-AES-CBC-CMAC-192	
id-PACE-ECDH-GM-AES-CBC-CMAC-256	
id-PACE-DH-IM-3DES-CBC-CBC	
id-PACE-DH-IM-AES-CBC-CMAC-128	
id-PACE-DH-IM-AES-CBC-CMAC-192	
id-PACE-DH-IM-AES-CBC-CMAC-256	
id-PACE-ECDH-IM-3DES-CBC-CBC	
id-PACE-ECDH-IM-AES-CBC-CMAC-128	
id-PACE-ECDH-IM-AES-CBC-CMAC-192	
id-PACE-ECDH-IM-AES-CBC-CMAC-256	
id-PACE-ECDH-CAM-AES-CBC-CMAC-128	
id-PACE-ECDH-CAM-AES-CBC-CMAC-192	
id-PACE-ECDH-CAM-AES-CBC-CMAC-256	
id-CA-DH-3DES-CBC-CBC	
id-CA-DH-AES-CBC-CMAC-128	
id-CA-DH-AES-CBC-CMAC-192	
id-CA-DH-AES-CBC-CMAC-256	
id-CA-ECDH-3DES-CBC-CBC	
id-CA-ECDH-AES-CBC-CMAC-128	
id-CA-ECDH-AES-CBC-CMAC-192	
id-CA-ECDH-AES-CBC-CMAC-256	
id-RI-DH-SHA-1	
id-RI-DH-SHA-224	
id-RI-DH-SHA-256	
id-RI-ECDH-SHA-1	
id-RI-ECDH-SHA-224	
id-RI-ECDH-SHA-256	
id-CAPA-ECDH-AES-CBC-CMAC-128	
id-CAPA-ECDH-AES-CBC-CMAC-192	
id-CAPA-ECDH-AES-CBC-CMAC-256	

If the eID Card under test supports Restricted Identification, the applicant SHALL provide all available private keys. There SHALL be at least one key with “authorized only” attribute set to YES and vice versa.

Note: For each key specified in this table, the test unit EAC2_ISO7816_R has to be performed.

Restricted Identification (public key)	Key ID	authorized only (YES or NO)

A.5 Additional Information

PIN	
Minimum PIN length	
PUK	
Default Retry Counter	
Invalid password reference for MSE:SetAT command at the beginning of PACE protocol (see Test case EAC2_ISO7816_H_23)	
Invalid private key reference for MSE:SetAT command at the beginning of CA protocol (see Test case EAC2_ISO7816_I_14)	
Command to send to the eID card to verify the chip's ability to still require Secured APDU. If not provided, use '00 B0 81 00 00'.	
Unsupported CAPA algorithm	
Date of Birth (for Smart-eID) in format YYMMDD	
Date of Expiration / Validity in format YYMMDD	
Valid Municipality ID	

A.6 PSA Information

The applicant has to provide following information about ps1-authInfo and ps2-authInfo in the PSAInfo supported by the eID card.

Supported ps1-authInfo and ps2-authInfo:

Data structure	Protocol	KeyId	ps1-authInfo value	ps2-authInfo value

PSA cipher suites:

Protocol Suite	Applicant declaration (YES or NO)
id-PSA-ECDH-ECSchnorr-SHA-256	
id-PSA-ECDH-ECSchnorr-SHA-384	
id-PSA-ECDH-ECSchnorr-SHA-512	

A.7 Initial External Authentication Information

The applicant has to provide the following information about protocol Initial External Authentication (IEA) supported by Smart-eID.

Key	Applicant declaration (in hex)
IEA Key ID (valid)	
IEA Key ID (invalid)	
IEA Private Key	