



Visa Europe

Visa Europe Technical Service Descriptions

June 2017



Notice: The Visa Europe Member Use Only label signifies that the information in this document is confidential and proprietary to Visa and is intended for use only by Visa Europe members, internal staff, and, where appropriate, other third parties that have a current nondisclosure agreement (NDA) with Visa Europe that covers disclosure of the information contained herein.

This document is protected by copyright restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorisation of Visa.

Changes are periodically added to the information herein. At any time, Visa Europe may make improvements and/or changes in the product(s) and/or the programme(s) that are described in this document.

Every reasonable effort has been made to ensure the accuracy of information provided by Visa Europe. Visa Europe shall not be held liable for any inaccurate information of any nature, however communicated by Visa Europe.

Visa and other trademarks are trademarks or registered trademarks of Visa.

All other product names mentioned herein are the trademarks of their respective owners.

© Visa Europe 2017

Contents

1	Introduction	23
1.1	Purpose	23
1.2	Audience	23
1.3	Scope	23
1.4	Summary of changes	23
1.5	Related information	23
2	Account Verification Service	24
2.1	Related information	24
2.2	Participation	24
2.2.1	Testing and certification	24
2.2.2	Service monitoring	24
2.2.3	Planning and implementation	24
2.3	How the service works	25
2.3.1	Card-present environment	25
2.3.2	Card-absent environment	25
2.3.3	Account verification process	25
2.3.4	Combined account and CVV2 or address verification process	26
2.4	Process flows	27
2.5	Message flows	28
2.6	Key messages	28
2.7	Key data fields	28
3	Acquirer Interchange Reporting Service	30
3.1	Related information	30
3.2	Participation	30
3.2.1	Planning and implementation	30
3.3	How the service works	30
3.4	Process flows	31
3.5	Key messages	32
3.6	Key fields	32
4	Address Verification Service	34
4.1	UK domestic service	34
4.2	Related information	34
4.3	Participation	34
4.3.1	Testing and certification	35
4.3.2	Service monitoring	35

4.3.3	Planning and implementation	35
4.4	How the service works	35
4.4.1	Verification data	36
4.4.2	Address verification data standards	36
4.4.3	Data compression	37
4.5	Process flows	38
4.6	Message flows	39
4.7	Key messages	40
4.8	Key data fields	40
5	Advice Retrieval Service - DMSA	42
5.1	Online retrieval	42
5.1.1	One station	43
5.1.2	Multiple stations	43
5.2	Offline retrieval	43
5.3	Related information	43
5.4	Participation	43
5.4.1	Testing and certification	43
5.4.2	Service monitoring	43
5.4.3	Planning and implementation	43
5.5	How the service works	45
5.5.1	DMSA advice message creation	45
5.5.2	Message processing modes	45
5.6	Process flows	46
5.6.1	DMSC advice delivery (offline)	47
5.6.2	Advice retrieval during and after a Visa Interchange Center switchover	48
5.7	Message flows	49
5.8	Key messages	50
5.9	Key data fields	51
6	Advice Retrieval Service - SMS	52
6.1	Online retrieval	52
6.1.1	One station	52
6.1.2	Multiple stations	53
6.2	Related information	53
6.3	Participation	53
6.3.1	Testing and certification	53
6.3.2	Service monitoring	53
6.3.3	Planning and implementation	53

6.4	How the service works	54
6.4.1	SMS advice message creation	54
6.4.2	Message processing modes	56
6.5	Process flows	57
6.5.1	Advice retrieval during and after a Visa Interchange Center switchover	58
6.6	Message flows	59
6.7	Key messages	59
6.8	Key data fields	61
7	ATM/POS Split Routing Service	62
7.1	Related information	62
7.2	Participation	62
7.2.1	Testing and certification	63
7.2.2	Planning and implementation	63
7.3	How the service works	63
7.3.1	ATM/POS Split Routing	63
7.3.2	ATM Account-Type Split Routing	63
7.3.3	Alternate Routing	63
7.4	Process flows	64
7.4.1	ATM/POS Split Routing process flow	65
7.4.2	ATM Account-Type Split Routing process flow	66
7.4.3	Alternate Routing option process flow	67
7.5	Message flows	69
7.6	Key data fields	69
8	Authorization Gateway Services	71
8.1	International Airline Program	72
8.2	Related information	72
8.3	Participation	72
8.3.1	Testing and certification	73
8.3.2	Available gateways	73
8.4	Process flows	76
8.5	Visa Gateway: Supported transaction types	77
9	Balance Inquiry Service	78
9.1	Related information	78
9.2	Participation	78
9.2.1	Issuer implementation considerations	78
9.2.2	Acquirer implementation considerations	79
9.2.3	Testing and certification	79

9.2.4	Service monitoring	79
9.2.5	Planning and implementation	79
9.3	How the service works	79
9.3.1	Stand-in processing	80
9.4	Message flow	81
9.5	Key messages	81
9.6	Key data fields	81
10	Bilateral Interchange Fee Processing Service	83
10.1	Related information	83
10.2	Participation	83
11	Card Recovery Bulletin Service	85
11.1	Related information	86
11.2	Participation	86
11.2.1	Testing and certification	86
11.2.2	Service monitoring	86
11.2.3	Planning and implementation	86
11.3	How the service works	86
11.3.1	Card recovery bulletin (CRB)	86
11.3.2	Regional Card Recovery File	88
11.3.3	Fees and billing reports	88
11.3.4	Exception File	88
11.3.5	Chargeback Reduction Service	90
11.3.6	Best practice	90
11.4	Process flow	91
11.4.1	CRB process flow	91
11.5	Key messages	92
11.6	Key data fields	92
12	Card Verification Service	94
12.1	Implementations	94
12.1.1	Basic processing principles	94
12.2	Related information	95
12.3	Participation	95
12.3.1	Participation requirements for Issuers:	95
12.3.2	Participation requirements for Acquirers	97
12.4	General Processing requirements	97
12.4.1	Additional processing requirements for dCVV	98
12.5	Requirements for checking card verification values	98

12.5.1	CVV, iCVV and dCVV	98
12.5.2	CVV2	98
12.6	Testing, monitoring and implementation requirements	99
12.6.1	Testing and certification	99
12.6.2	Service monitoring	99
12.6.3	Planning and implementation for an Issuer	99
12.6.4	Planning and implementation for an Acquirer	99
12.6.5	Ongoing maintenance and enhancement of the Card Verification Service ...	100
12.7	How the service works	100
12.7.1	Service code	101
12.7.2	Expiry date	101
12.7.3	dynamic Card Verification Value (dCVV)	102
12.7.4	Emergency replacement cards	102
12.8	Process flow	103
12.9	Message flows	104
12.9.1	Card Verification Value (CVV)	104
12.9.2	Integrated Chip Card Verification Value (iCVV)	105
12.9.3	Card Verification Value 2 (CVV2)	106
12.9.4	Dynamic Card Verification Value (dCVV)	107
12.10	Key messages	107
12.11	Key data fields	108
13	Chargeback Reduction Service	110
13.1	Acquirer benefits	110
13.2	Issuer benefits	110
13.3	Participation	110
13.4	Related information	110
13.5	How the service works	111
13.5.1	Validating POS transactions	111
13.5.2	Validating chargebacks	111
13.5.3	Adding status indicators	113
13.5.4	Advice messages and reports	115
13.6	Process flows	116
14	Cross-Border Domestic Interchange Program	117
14.1	Related information	117
14.2	Participation	117
14.2.1	Testing	117
14.3	How the service works	118

14.3.1	Registering Merchants on VOL	118
14.3.2	VECSS processing	118
14.4	Process flow	119
14.5	Key messages	119
14.5.1	Authorization	119
14.5.2	Clearing	120
14.6	Key data fields	120
15	Currency Conversion Service	121
15.1	Related information	122
15.2	Participation	122
15.3	How the service works	122
15.3.1	Understanding decimal positioning	123
15.3.2	How currency conversions are calculated	124
15.3.3	Charging an Optional Issuer Fee	124
15.3.4	Choosing the Settlement Currency	124
15.4	How buy and sell currency rates are applied to transactions	124
15.4.1	Understanding rate-related terminology	125
15.4.2	How rate pairs are determined	126
15.4.3	How buy and sell rates are applied	126
15.5	Currency conversion process in brief	127
15.6	Examples of currency conversions	128
15.7	Currency Rate Delivery Service	129
15.8	Enhanced Interchange Data Service	130
15.8.1	Transaction types used by the Enhanced Interchange Data Service	131
15.9	Key messages and data fields	131
16	Custom Payment Service/ATM	132
16.1	Related information	132
16.2	Participation	132
16.2.1	Requirements for ATM Acquirers	133
16.2.2	Requirements for ATM Issuers	133
16.2.3	Testing and certification	133
16.2.4	Service monitoring	133
16.2.5	Planning and implementation	133
16.3	How the service works	134
16.3.1	CPS/ATM qualification requirements for authorization	136
16.3.2	CPS/ATM qualification requirements for clearing	136
16.3.3	Further Clearing checks	137

16.4	Process flows	137
16.4.1	Process flow for CPS/ATM authorization	138
16.4.2	Process flow for CPS/ATM clearing	138
16.5	Message flows	139
16.6	Key data fields	140
16.6.1	Key field cross reference	140
17	Euro Area Net Settlement Service	144
17.1	Related information	144
17.2	Participation	144
17.3	How the service works	144
17.3.1	Clearing and settlement timing	145
17.3.2	Funds transfer	145
17.4	Process flows	146
18	File Collection and Delivery Service	147
18.1	Related information	147
18.2	Participation	147
18.2.1	Planning and implementation	147
18.2.2	Testing and certification	147
18.2.3	Service monitoring	148
18.3	How the service works	148
18.3.1	File collection	148
18.3.2	File delivery	148
18.4	Process flows	151
18.4.1	Process flows for collection	152
18.4.2	Process flows for delivery	152
19	Fraud Reporting System	155
19.1	Related information	155
19.2	Participation	155
19.2.1	Testing and certification	156
19.2.2	Service compliance	156
19.2.3	Planning and implementation	156
19.3	How the service works	156
19.3.1	Reporting fraud correctly	157
19.3.2	Checking the status of reported fraud transactions	158
19.3.3	Correctly submitted fraud transactions	160
19.3.4	Incorrectly submitted fraud transactions	160
19.4	Process flows	161

19.5	Message flows	161
19.5.1	Message flow for Members that send TC 40 Fraud Advice transactions	161
19.5.2	Message flow for Members that send 9620 Fraud Advice messages	162
19.6	Key messages	164
20	Interchange Reimbursement Fee Processing Service	165
20.1	Enhanced Interchange Data Service	165
20.2	Related information	165
20.3	Participation	165
20.4	How the service works	166
20.4.1	Enhanced Interchange Data Service	167
20.5	Process flow	168
20.6	Key data fields	168
21	International Settlement Service	170
21.1	Related information	170
21.2	Participation	170
21.3	How the service works	170
21.3.1	Clearing and settlement timing	171
21.3.2	Funds transfer	171
21.4	Process flow	173
22	Multicurrency Service	174
22.1	Related information	174
22.2	Participation	175
22.3	How the service works	175
22.3.1	Visa Europe System acquired MasterCard transactions	177
22.3.2	Understanding decimal positioning	177
22.3.3	How currency conversions are calculated	178
22.3.4	Charging an Optional Issuer Fee	178
22.3.5	Choosing the Settlement Currency	179
22.4	How buy and sell currency rates are applied to transactions	179
22.4.1	Understanding rate-related terminology	179
22.4.2	How rate pairs are determined	181
22.4.3	How buy and sell rates are applied	181
22.5	Currency conversion process in brief	182
22.5.1	Examples of currency conversions	183
22.6	Currency Precision Service	184
22.6.1	Currency Precision Service for Acquirers	185
22.6.2	Currency Precision Service for Issuers	186

22.6.3	One position decimal adjustment	186
22.6.4	Two position decimal adjustment	187
22.7	Currency Rate Delivery Service	188
22.8	Enhanced Interchange Data Service	188
22.8.1	Transaction types used by the Enhanced Interchange Data Service	189
22.9	VEAS: Key messages for the Multicurrency Service	189
22.10	VEAS: Key data fields used by the Multicurrency Service	189
22.11	DMSC: Key messages and fields used by the Multicurrency Service	191
22.12	Multicurrency transaction examples	191
22.12.1	Example 1 - DMSA purchase transaction	191
22.12.2	Example 2 - SMS purchase transaction	192
22.12.3	Example 3 - SMS ATM cash withdrawal and balance inquiry	193
23	National Net Settlement	195
23.1	Related information	195
23.2	Participation	195
23.3	How the service works	196
23.3.1	Clearing and settlement timing	196
23.3.2	Funds transfer	196
24	Partial Authorization	198
24.1	Related information	198
24.2	Participation	198
24.2.1	Issuer implementation considerations	198
24.2.2	Acquirer implementation considerations	198
24.2.3	Testing and certification	199
24.3	How the service works	199
24.3.1	Reversals	201
24.3.2	Prepaid cards	201
24.4	Message flow	202
24.5	Key messages	203
24.6	Key data fields	204
25	PIN Management Service	205
25.1	Related information	205
25.2	Participation	205
25.2.1	Issuer implementation considerations	205
25.2.2	Acquirer implementation considerations	205
25.2.3	Testing and certification	205
25.2.4	Service monitoring	206

25.2.5	Planning and implementation	206
25.3	How the service works	206
25.3.1	Stand-in processing	207
25.4	Process flow	208
25.5	Message flow	209
25.6	Key messages	209
25.7	Key data fields	209
26	PIN Routing Service	211
26.1	Related information	211
26.2	Participation	211
26.2.1	Testing and certification	211
26.2.2	Planning and implementation	212
26.3	How the service works	212
26.3.1	PIN/No-PIN Split Routing option	212
26.3.2	POS PIN Routing option	212
26.4	Process flows	212
26.4.1	PIN/No-PIN Split Routing option process flow	212
26.4.2	POS PIN Routing option process flow	213
26.5	Message flows	214
26.5.1	PIN/No-PIN Split Routing option message flow	214
26.5.2	POS PIN Routing option message flow	215
26.6	Key data fields	216
27	PIN Verification Service	218
27.1	Related information	218
27.2	Participation	219
27.2.1	Issuer requirements	219
27.2.2	Testing and certification	219
27.2.3	Service monitoring	219
27.2.4	Planning and implementation	220
27.3	How the service works	220
27.3.1	PIN Verification Value method	222
27.3.2	IBM PIN offset method	223
27.4	Process flow	224
27.5	Message flow	226
27.6	Key messages	227
27.7	Key data fields	227

28	Positive Cardholder Authorization Service	230
28.1	Related information	230
28.2	Participation	230
28.2.1	Issuer and activity limits	230
28.2.2	Service monitoring	231
28.2.3	Planning and implementation	231
28.3	How the service works	231
28.3.1	Routing	231
28.3.2	Stand-in processing	231
28.3.3	PCAS parameters	232
28.3.4	Merchant category groups	233
28.3.5	Issuer limits	233
28.3.6	Advice limits	234
28.3.7	Activity limits	235
28.3.8	Mandated minimum limits	237
28.3.9	Activity checking	239
28.3.10	Cardholder risk levels and individual limits	241
28.3.11	Random selection factors	243
28.3.12	BIN blocking, country restrictions, risky countries and country-to-country embargos	243
28.3.13	Suppress inquiry mode	244
28.4	Key data fields	244
29	Priority Routing Service	245
29.1	Related information	245
29.2	Participation	245
29.2.1	Testing and certification	246
29.2.2	Planning and implementation	246
29.3	How the service works	246
29.4	Process flows	247
29.5	Message flows	248
29.6	Key data fields	248
30	Real Time Scoring Service	249
30.1	Related information	249
30.2	Participation	249
30.3	How the service works	250
30.3.1	Using the score only option	250
30.3.2	Using the Real Time Scoring full solution	251

30.4	Process flows	251
30.4.1	Process flow for the RTS score only option	252
30.4.2	Process flow for the RTS full solution option	253
30.5	Message flows	257
30.6	Key data fields	257
31	Verified by Visa Service	258
31.1	Related information	259
31.2	Participation	259
31.2.1	Issuer requirements	259
31.2.2	Acquirer requirements	260
31.2.3	Testing and certification	260
31.2.4	Service monitoring	260
31.2.5	Planning and implementation	260
31.3	How the service works	262
31.3.1	Linking three domains	262
31.4	Process flow	263
31.5	Message (authorization) flow	264
31.6	Key messages	266
31.6.1	Verify enrolment	266
31.6.2	Payer authentication	266
31.6.3	Authentication history	266
31.6.4	CAVV validation	267
31.7	Key data fields	267
32	Visa Alternative Authorization Routing	268
32.1	Related information	268
32.2	Participation	268
32.2.1	Acquirer participation	268
32.2.2	Issuer participation	268
32.2.3	Planning and implementation	268
32.2.4	Testing and certification	268
32.3	How the service works	269
32.4	Process flow	269
32.5	Key messages	270
32.6	Key data fields	270
33	Visa cash back Service	271
33.1	Related information	271
33.2	Participation	271

33.2.1	Standard and domestic operating parameters	272
33.2.2	Issuer implementation considerations	273
33.2.3	Acquirer implementation considerations	274
33.2.4	Testing and certification	274
33.2.5	Service monitoring	275
33.2.6	Planning and implementation	275
33.3	How the service works	275
33.3.1	Stand-in processing	277
33.3.2	Exception processing - chargebacks	277
33.3.3	Chip card data	277
33.3.4	UK cash back Service	277
33.4	Process flow	278
33.5	Message flow	278
33.6	Key messages	279
33.7	Key data fields	279
34	Visa Device Profiling	281
34.1	Related information	281
34.2	Participation	281
34.2.1	Planning and implementation	281
34.3	How the service works	281
34.3.1	Subscription and access rights	282
34.4	Reports delivered by VDP	282
34.4.1	Strategic reports	282
34.4.2	Operational reports	283
35	Visa Europe Payment Stop Service	284
35.1	Related information	284
35.2	Participation	284
35.2.1	Impact considerations for Acquirers	285
35.2.2	Impact considerations for Issuers	285
35.2.3	Planning and implementation	285
35.3	How the service works	286
35.3.1	Levels of payment stop instructions	286
35.3.2	Transaction eligibility	286
35.3.3	Interaction with other services	286
35.4	Process flow	287
35.5	Message flows	288
35.6	Key messages	289

35.6.1	Authorization	289
35.6.2	Clearing	289
35.7	Key data fields	289
35.7.1	Authorization	289
35.7.2	Clearing	290
36	Visa Member Testing Service for VEAS	291
36.1	Visa Member Testing Service for VEAS and production differences	291
36.2	Related information	291
36.3	Participation	292
36.3.1	Planning and implementation	292
36.4	How the service works	294
36.4.1	Member self-testing	294
36.4.2	Testing with a Technical Implementation Consultant	295
36.4.3	Message testing	296
37	Visa Member Testing Service for VECSS	297
37.1	Visa Member Testing Service for VECSS and production differences	297
37.2	Related information	297
37.3	Participation	297
37.3.1	Planning and implementation	298
37.4	How the service works	301
37.4.1	Batch Responder environment	302
37.4.2	Responder BINs	303
38	Visa Payment Controls	304
38.1	Related information	304
38.2	Participation	304
38.3	How the service works	304
38.3.1	Interfaces and user roles	305
38.3.2	Card rules	305
38.3.3	VEAS processing	307
38.3.4	Customer support	307
38.4	Process flows	307
38.5	Key messages	308
38.6	Key data fields	308
39	Visa Shortest Online Path Service	309
39.1	Related information	309
39.2	Participation	309
39.2.1	Testing and certification	309

39.2.2	Planning and implementation	309
39.3	How the service works	310
40	Visa Smart Debit/Credit Service	311
40.1	Related information	311
40.2	VSDC features	312
40.2.1	Card types	314
40.2.2	VSDC supporting services	315
40.3	Participation	315
40.3.1	Requirements for Acquirers	315
40.3.2	Requirements for Issuers	316
40.3.3	Testing and certification	316
40.3.4	Service monitoring	316
40.3.5	Planning and implementation	316
40.4	How the service works	316
40.4.1	A - Approve offline	319
40.4.2	B - Decline offline	319
40.4.3	C - Online authorization required	320
40.4.4	DMSA routing and STIP	321
40.4.5	SMS routing and STIP	321
40.4.6	Fallback transaction	321
40.5	Process flow	322
40.6	Key messages	322
40.7	Key data fields	323
41	Visa Token Service	325
41.1	Related information	326
41.2	Participation	326
41.2.1	Acquirer participation	326
41.2.2	Issuer participation	326
41.2.3	Testing and certification	327
41.3	How the service works	327
41.3.1	Service enrolment	327
41.3.2	Payment token provisioning	328
41.3.3	Transaction processing	329
41.3.4	Payment token lifecycle management	329
41.4	Process flows	330
41.4.1	Obtaining a payment token	330
41.4.2	Making a payment using Visa payWave for mobile devices	331

41.4.3	Making an application-based e-commerce purchase	331
41.5	Key Visa Europe System messages	332
41.5.1	Authorization	332
41.5.2	Clearing	332
41.6	Key data fields	333

Tables

Table 1:	Fields contained in the Acquirer Interchange Report	32
Table 2:	Examples of the effect of different data compression methods	37
Table 3:	Deferred clearing advice messages	55
Table 4:	Gateways available to DMSA Members	73
Table 5:	Visa Gateway: Supported transaction types	77
Table 6:	Account number listing dependencies	87
Table 7:	Exception File action codes	89
Table 8:	CRB service regions	89
Table 9:	Processing options for CVV, iCVV, dCVV and CVV2	96
Table 10:	Reasons Edit Package rejects a chargeback	112
Table 11:	Conditions under which CRS returns invalid chargebacks to Issuers	113
Table 12:	Examples of decimal positioning	123
Table 13:	Rate-related terminology	125
Table 14:	Rate-related terminology mapped to fields in DMSC message	126
Table 15:	Formulae for converting currencies	127
Table 16:	Examples of currency conversions	129
Table 17:	CPS/ATM qualification requirements for authorization	136
Table 18:	CPS/ATM qualification requirements for clearing	137
Table 19:	Edit level checks for CPS/ATM transactions	137
Table 20:	Custom Payment Service/ATM - key field cross reference	141
Table 21:	Options for file delivery	149
Table 22:	Customised delivery file types	150
Table 23:	Split routing codes	151
Table 24:	FRS status of reported transactions	158
Table 25:	FRS report options	159
Table 26:	How jurisdiction of a transaction is determined	166
Table 27:	Examples of decimal positioning	178
Table 28:	Rate-related terminology	179

Table 29: Mapping of rate-related terms to fields in DMSC messages	180
Table 30: Examples of currency conversions	184
Table 31: Currency Precision Service - applicable fields	185
Table 32: Merchant category groups	233
Table 33: Issuer limits	234
Table 34: Advice limits	234
Table 35: Cardholder activity limits	235
Table 36: Visa-mandated minimum Issuer limits for International Transactions	238
Table 37: Visa-mandated minimum 1-day activity limits for International Transactions: Issuer available	238
Table 38: Visa-mandated minimum 1-day activity limits for International Transactions: Issuer unavailable	238
Table 39: Issuer limits	239
Table 40: Activity limits	239
Table 41: Pass and fail parameters for MCG activity checks	240
Table 42: PCAS parameters in Risk File	241
Table 43: RTS solutions	250
Table 44: Cash back services supported by Visa Europe	271
Table 45: Visa cash back Service - Standard and domestic operating parameters	272
Table 46: Response and reject codes	274
Table 47: Cash back fail conditions and corresponding processing rules	276
Table 48: VPC interfaces and users	305
Table 49: VPC Rules	306

Figures

Figure 1: Process flow for the Account Verification Service	27
Figure 2: Message flow for the Account Verification Service	28
Figure 3: Process flow for Acquirer Interchange Reporting Service	31
Figure 4: Process flow for the Address Verification Service	38
Figure 5: Message flow for the Address Verification Service	39
Figure 6: Message flow for a combined authorization and address verification	40
Figure 7: Process flow for the DMSA Advice Retrieval Service	46
Figure 8: Message flows for the DMSA Advice Retrieval Service	49
Figure 9: Process flow for the SMS Advice Retrieval Service	57
Figure 10: Message flows for the SMS Advice Retrieval Service	59
Figure 11: Process flow for ATM/POS Split Routing	65

Figure 12: Process flow for ATM Account-Type Split Routing	66
Figure 13: Process flow for Alternate Routing option	68
Figure 14: Message flow for the Alternate Routing	69
Figure 15: Process flow for the Authorization Gateway Services	76
Figure 16: Message flow for the Balance Inquiry Service	81
Figure 17: Chart showing the production date and effective periods for bulletins 92-94	87
Figure 18: CRB process flow	91
Figure 19: Key messages for the Card Recovery Bulletin Service	92
Figure 20: How the Card Verification Service works	101
Figure 21: Message flow for the Card Verification Service using CVV	104
Figure 22: Message flow for the Card Verification Service using iCVV	105
Figure 23: Message flow for the Card Verification Service using CVV2	106
Figure 24: Message flow for the Card Verification Service using dCVV	107
Figure 25: Process flow for Acquirers using the CRS	116
Figure 26: Process flow for Issuers using the CRS	116
Figure 27: Clearing and settling a multicurrency transaction	123
Figure 28: Triangulation - Acquirer to Issuer	127
Figure 29: Conversion of source amount to TADC	128
Figure 30: Overview of how CPS/ATM works	134
Figure 31: Process flow for CPS/ATM authorization	138
Figure 32: Process flow for CPS/ATM clearing	138
Figure 33: Message flow for CPS/ATM authorization in a DMSA environment	139
Figure 34: Process flow for the Euro Area Net Settlement Service	146
Figure 35: Process flow for standard collection	152
Figure 36: Process flow for standard delivery	152
Figure 37: Process flow for delivery by volume	153
Figure 38: Process flow for customised delivery	153
Figure 39: Example of split routing	154
Figure 40: Process flow for the FRS	161
Figure 41: Message flow for Members that send TC 40 Fraud Advice transactions	162
Figure 42: Message flow for Members that send 9620 Fraud Advice messages	163
Figure 43: Process flow for the Interchange Reimbursement Fee Processing Service	168
Figure 44: Process flow for the International Settlement Service	173
Figure 45: Authorizing a multicurrency transaction	176
Figure 46: Clearing and settling a multicurrency transaction	177
Figure 47: Triangulation - Acquirer to Issuer	182

Figure 48: Conversion of TADC to destination currency	183
Figure 49: Multicurrency transaction example 1	192
Figure 50: Multicurrency transaction example 2	193
Figure 51: Multicurrency transaction example 3	194
Figure 52: Message flow for the Partial Authorization Service	203
Figure 53: Process flow for the PIN Management Service	208
Figure 54: Message flow for the PIN Management Service	209
Figure 55: Process flow for PIN/No-PIN Split Routing option	213
Figure 56: Process flow for POS PIN Routing option	214
Figure 57: Message flow for PIN/No-PIN Split Routing option	215
Figure 58: Message flow for POS PIN Routing option	216
Figure 59: How the PIN Verification Service works	221
Figure 60: Process flow for the PIN Verification Service	224
Figure 61: Message flow for the PIN Verification Service when PIN is valid	226
Figure 62: Message flow for the PIN Verification Service when PIN is declined	227
Figure 63: Process flow for the Priority Routing Service	247
Figure 64: Message flow for the Priority Routing Service	248
Figure 65: Process flow for the RTS score only option	252
Figure 66: Process flow for the RTS full solution	253
Figure 67: RTS full solution with risk score	254
Figure 68: RTS full solution with decision recommendations	255
Figure 69: RTS full solution with authorization decision-making	256
Figure 70: Message flow for the RTS service	257
Figure 71: Process flow for the Verified by Visa Service	263
Figure 72: Message (authorization) flow for the Verified by Visa Service	265
Figure 73: Visa Alternative Authorization Routing process flow	269
Figure 74: Process flow for the Visa cash back Service	278
Figure 75: Message flow for the Visa cash back Service	278
Figure 76: Process flow for the payment stop service	287
Figure 77: Message flow for an authorization request declined by the payment stop service	288
Figure 78: Message flow for a Clearing record returned by the payment stop service	289
Figure 79: Using VMTS to test the Acquirer role	295
Figure 80: Using VMTS to provide a STIP response	296
Figure 81: The Batch Responder environment	302
Figure 82: How the VSDC Service works	317

Figure 83: Online authorization for the VSDC Service	320
Figure 84: Process flow for the VSDC Service	322

1 Introduction

1.1 Purpose

This manual provides a description of each service, how it works, and details the conditions and prerequisites required of Members to support it.

1.2 Audience

This manual is for business and technical managers who are responsible for the planning and implementation of Visa Europe services.

Technical staff who are responsible for implementing and configuring Visa Europe services are expected to read the more detailed processing and technical specifications.

1.3 Scope

This manual outlines the technical processes involved in using each service, plus the testing, certification and implementation requirements.

Detailed technical and processing information is outside the scope of this guide. For more information see the Visa Europe technical and processing specifications.

1.4 Summary of changes

The following service descriptions have been updated:

- Advice Retrieval Service - DMSA
 - Clarifications and removal of obsolete 0800 message codes
- Partial Authorization
 - AFD Issuer Mandate
- Visa Payment Controls
 - Updated description to include version 2 functionality

1.5 Related information

See the *Visa Europe System Manuals: Quick Start Guide* for a summary of all available system manuals.

See the *Visa Acronyms Quick Reference* document for the meanings of Visa acronyms and abbreviations.

For further information, you can also visit our website or contact us:

- For information about Visa Europe: www.visaeurope.com
- For Member documentation: www.eu.visaonline.com
- For questions or comments about this document: customersupport@visa.com

2 Account Verification Service

The Account Verification Service enables a Merchant to verify a Visa account by submitting an authorization request for a Transaction Amount of zero. This is also referred to as an account verification check.

In the card-absent environment, Acquirers use the service to verify an account, either as an account verification check only, or in conjunction with Card Verification Value 2 (CVV2), or Cardholder billing address (Address Verification Service) checks.

Account verification requests are forwarded directly to the Issuer.

2.1 Related information

For further information about the Account Verification Service, see the following documents:

- *Dual Message System Authorization (DMSA) Processing Specifications*
- *Single Message System (SMS) POS Processing Specifications*
- *Visa Europe Merchant Data Standards*

2.2 Participation

The Account Verification Service is available through the dual and single messaging systems.

Participation is:

- Mandatory for Issuers
- Optional for Acquirers and Merchants

To participate in the service, Members must meet the following requirements.

2.2.1 Testing and certification

Certification is mandatory for participation in the service. Visa Member Testing Service (VMTS) provides testing and certification assistance. To arrange for testing and certification, Members must contact Visa Europe Customer Support.

2.2.2 Service monitoring

Members may be eligible for compliance monitoring. For more information, Members must contact Visa Europe Customer Support.

2.2.3 Planning and implementation

For more information, Members must contact Visa Europe Customer Support.

2.3 How the service works

An account verification can be sent in card-present environments and card-absent environments.

2.3.1 Card-present environment

A successful verification confirms that a transaction can be completed using the card.

Such verifications are based on validating the account number only, but additional address and CVV2 validation may also be requested.

2.3.2 Card-absent environment

In a card-absent environment, the Cardholder and Merchant are in different locations, therefore, the card is not available to the Merchant. For example, when a Cardholder sets up an account with an internet supplier, mail/phone order Merchant, or T&E Merchant. In addition to supplying the card number, the Cardholder is usually asked for (or prompted to enter) details of the address pertinent to the card, or the card's CVV2 number.

2.3.3 Account verification process

In this example, a Merchant verifies an account using only the account number:

1. Merchant sends a zero value Transaction Amount to the Acquirer.
2. The Acquirer creates a zero value authorization request and sends it to VEAS.
 - A 0100 message is sent by users of dual message processing and SMS
 - The authorization message is populated as an account verification request

Authorization request			
Field	Name	Value	Description
2	Primary Account Number	n(n)	Account number of the Cardholder
4	Amount, Transaction	0(12)	Must indicate a Transaction Amount of zero
18	Merchant Type	n(4)	Any code except: 5542 (Automated Fuel Dispensers) 6011 (ATM)
25	Point-of-Service Condition Code	51	Account verification (no financial authorization request)

3. VEAS forwards the authorization request with a Transaction Amount of zero, directly to the Issuer.
 - The request is always sent to the Issuer. Stand-in processing (STIP) is only invoked if the Issuer is unavailable.
 - If STIP is invoked, the modulus-10 check digit and Exception File are checked. STIP generates an authorization response, based on the outcome of these checks.

4. The Issuer evaluates the authorization request and sends an authorization response to VEAS.
 - The Issuer checks that the account is a valid account number, and that the account is open and has not been listed for pickup. If the account is in good standing, the Issuer responds that there is no reason to decline the service.
 - A positive verification does not necessarily reserve funds in the Cardholder's account.

Data field 39, response code			
Field	Name	Value	Description
39	Response Code	85	No reason to decline

5. VEAS edits the authorization response and forwards the response to the Acquirer.
6. The Acquirer routes the authorization response to the Merchant.
7. The Merchant gains assurance regarding account validity.

2.3.4 Combined account and CVV2 or address verification process

In a card-absent environment, a Merchant verifies an account using the supplied account number, and CVV2 and/or Cardholder billing address:

1. Merchant sends an authorization request with a Transaction Amount of zero to the Acquirer.
 - Account number, and CVV2 and/or address as quoted or entered by Cardholder
2. Acquirer creates an authorization request with a Transaction Amount of zero and sends it to VEAS.
 - A 0100 message is sent by users of dual message processing and SMS
 - The authorization message is populated as an account verification request

Authorization request			
Field	Name	Value	Description
2	Primary Account Number	n(n)	Account number quoted by Cardholder
4	Amount, Transaction	0(12)	Must indicate zero amount
18	Merchant Type	n(4)	Merchant's business category
25	Point-of-Service Condition Code	51	Account verification
123	Verification Data	xxx	Address quoted by Cardholder
126.10	CVV2 Authorization Request Data	n(3)	CVV2 number quoted by Cardholder

3. VEAS forwards the authorization request with a Transaction Amount of zero directly to the Issuer. Depending on the Issuer's CVV2 validation options, VEAS may validate the CVV2 before forwarding the request to the Issuer.
 - The request is always sent to the Issuer. STIP is only invoked if the Issuer is unavailable.

- The CVV2 code can only be verified by VEAS if the relevant encryption keys are available to Visa. If they are not, the code can only be verified by the Issuer.
 - If the Issuer is unavailable, the address cannot be verified: STIP cannot process an address verification
4. Issuer evaluates the request and sends an authorization response to VEAS.
- The Issuer checks the account number, address and CVV2 as appropriate, and if no issues are found, confirms the card's validity.

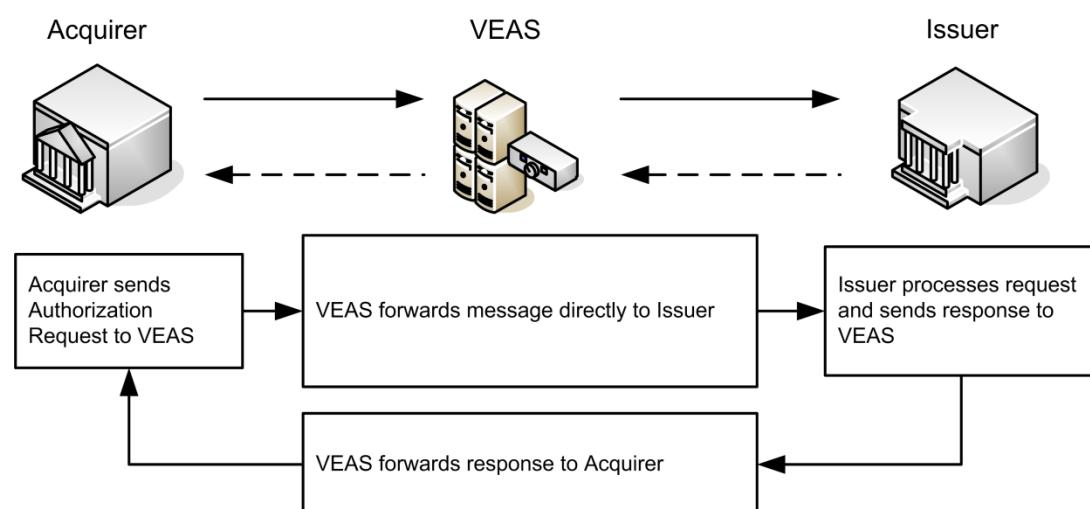
Authorization response			
Field	Name	Value	Description
39	Response Code	85	No reason to decline
44.2	Address Verification Results Code	Multiple	See <i>Address Verification Service</i>
44.10	CVV2 Result Code	Multiple	See <i>Card Verification Service</i>

5. VEAS edits the authorization response and forwards the response to the Acquirer.
6. The Acquirer routes the authorization response to the Merchant.
7. The Merchant gains assurance regarding account validity.

2.4 Process flows

The process flow for the Account Verification Service follows standard message routing, as illustrated in the following diagram.

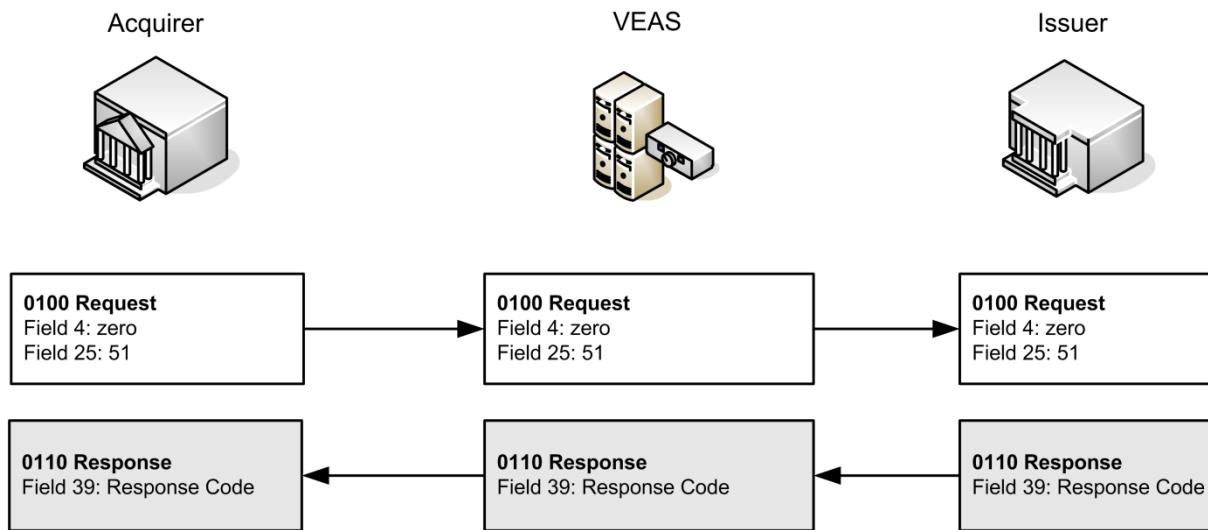
Figure 1: Process flow for the Account Verification Service



2.5 Message flows

The following diagram illustrates the message flow for account verification.

Figure 2: Message flow for the Account Verification Service



2.6 Key messages

The following messages carry the Account Verification Service:

- 0100 authorization request
- 0110 authorization response
- 0200 full financial request
- 0210 full financial response

2.7 Key data fields

The following key data fields are used by the Account Verification Service. For detailed information, see the Visa Europe technical specifications.

Data field 2 - Primary Account Number

This data field contains the account number of the Cardholder.

Data field 4 - Amount, Transaction

This data field contains an amount that must be zero.

Data field 18 - Merchant Type

This data field contains the Merchant type code, also known as the Merchant Category Code (MCC). For an account verification, this cannot be 5542 (Automated Fuel Dispensers) or 6011 (ATM).

Data field 25 - Point-Of-Service Condition Code

This data field contains the POS condition code included in the verification request. The code must be set to:

51 - Account Verification

Data field 39 - Response Code

This data field contains a code indicating the Issuer's response. If the account is valid and there are no recognised issues, the response code is:

85 - No reason to decline

Data field 44.1 - Response Source

This data field indicates whether the verification was carried out by the Issuer or by STIP.

3 Acquirer Interchange Reporting Service

The Acquirer Interchange Reporting Service provides Acquirers with transaction level reporting containing interchange fee related information for Visa Europe processed point-of-sale (POS) transactions. The service assists Acquirers in fulfilling their obligations under Article 12 of the EU Interchange Fee Regulation (IFR).

Article 12 of the IFR describes a requirement that, after the execution of a card-based payment transaction, the payee's payment service provider (the Acquirer) shall make available to the payee (the Merchant) transaction level reporting which includes the Interchange Reimbursement Fee amount.

Acquirers can subscribe one or more of their Business ID (BIDs) to the service and receive daily reports containing POS non-cash transactions acquired by BINs linked to these subscribed BIDs and cleared through the Visa Europe Clearing and Settlement Service (VECSS). There is one report for each subscribed BID.

When subscribing, an Acquirer can opt to receive an extra initial report that details historical transaction data going back 3 months.

3.1 Related information

The following documents contain further information about the Acquirer Interchange Reporting Service:

- *Acquirer Interchange Reporting Member Implementation Guide*
- *Acquirer Interchange Reporting Member Implementation Questionnaire*
- *Visa File Transfer Initial Setup Guide*
- *Dual Message System Clearing (DMSC) Technical Specifications*
- *Single Message System (POS) Technical Specifications*

3.2 Participation

Participation in the service is optional for Acquirers.

3.2.1 Planning and implementation

Members that choose to participate in the Acquirer Interchange Reporting Service undergo an onboarding process. Onboarding is the process of successfully integrating a new entity to the service. For more information, see the *Acquirer Interchange Reporting Member Implementation Guide*.

3.3 How the service works

Members that subscribe to the service receive a daily transaction level report via the Visa File Transfer service (VFT). Data for each Visa Europe processed POS transaction from the subscribing Acquirer is present in the report. The report is delivered in the form of a data file

and includes the following:

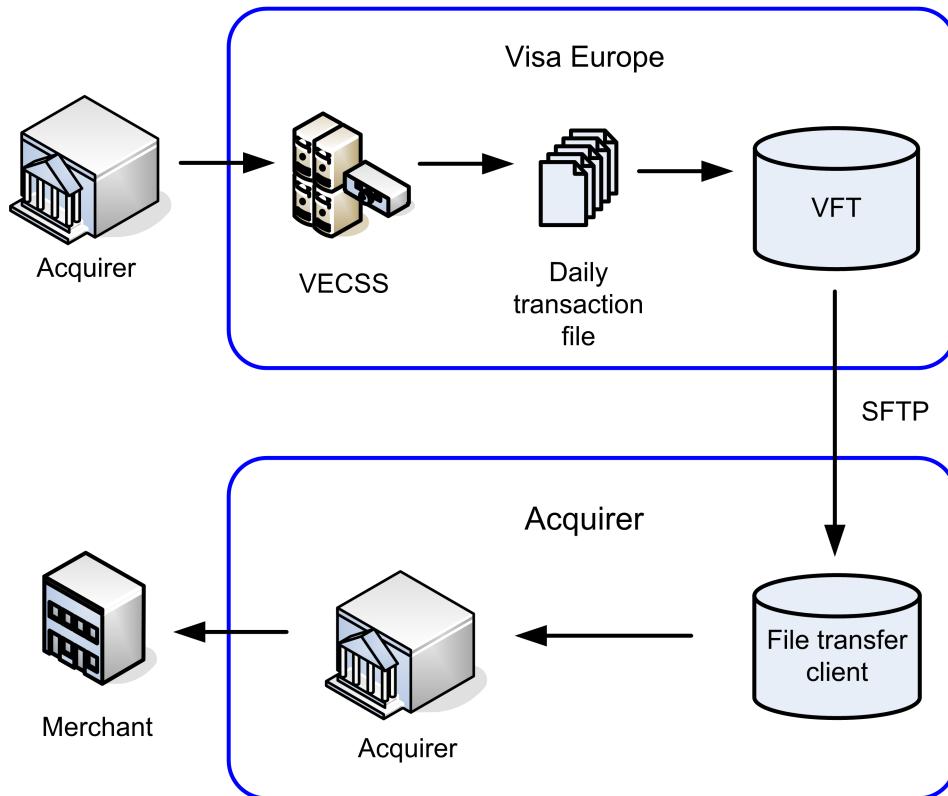
- Transaction identification data
- Settled interchange fee amount and fee descriptor
- Transaction amount
- Card product information
- Merchant information

VFT uses a Secure File Transfer Protocol (SFTP) connection to transfer data in an encrypted format. For more information about VFT, see the *Visa File Transfer Initial Setup Guide*.

3.4 Process flows

This section gives a high-level overview of the process flow involved in the Acquirer Interchange Reporting Service.

Figure 3: Process flow for Acquirer Interchange Reporting Service



1. VECSS collects Clearing files from Acquirers on a daily basis.
2. VECSS generates a transaction file containing all the Acquirer's POS transactions, including the interchange fee applied to each transaction.
3. Visa Europe uses the VFT service to deliver the file to the Acquirer's file transfer client via SFTP.
4. Acquirer combines their data with the Visa data and makes reporting available to their Merchant.

3.5 Key messages

The following are the key Clearing records for the service:

- TC05, Sales Draft or Representment
- TC06, Credit Voucher or Merchandise Return
- TC15, Sales Draft Chargeback
- TC16, Credit Voucher Chargeback
- TC25, Sales Draft Reversal
- TC26, Credit Voucher Reversal
- TC35, Sales Draft Chargeback Reversal
- TC36, Credit Voucher Chargeback Reversal

For detailed information, see the Visa Europe technical specifications.

3.6 Key fields

The following table lists the fields that appear in the Acquirer Interchange Reporting Service report.

Table 1: Fields contained in the Acquirer Interchange Report

Name	Description
Central Processing Date (CPD)	The date Visa Europe Clearing and Settlement Service (VECSS) processed the transaction TCR 0, Positions 164-167
Acquirer BIN	The BIN used to process the transaction TCR 0: Positions 28-33 (Acquirer Reference Number subfield)
Transaction Code	Transaction type TCR 0, Positions 1-2
Transaction Code Qualifier	Identifies AFT and OCT transactions TCR 0, Position 3
Usage Code	Identifies representment transactions TCR 0, Position 147
Acquirer Reference Number(ARN)	Transaction reference TCR 0, Positions 27-49
Source Amount	The submitted transaction amount in source currency TCR 0, Positions 77-88
Source Currency Code	The currency of the source amount TCR 0, Positions 89-91 (ISO numeric)
Cashback Amount	If the transaction includes cashback, the cashback amount in source currency will be included TCR 1, Positions 158-166

Table 1: Fields contained in the Acquirer Interchange Report (continued)

Name	Description
Acquirer Settlement Amount	Transaction amount in the Acquirer's settlement currency
Acquirer Settlement Currency Code	The currency of the Acquirer Settlement Amount and Interchange Amount
Interchange Fee Amount	The calculated interchange fee in the acquirer's settlement currency (rounded to 6 decimal places as calculated in VECSS)
Interchange Fee Descriptor	The descriptor for the interchange fee at which the transaction was settled
Interchange Fee Sign (credit or debit)	Whether the interchange fee amount was credited to or debited from the acquirer
Product ID	Product ID of the account number used in the transaction TCR 5, Positions 136-137
Account Funding Source	Account funding source of the account number used in the transaction
Product Sub-Type	Product sub-type of the account number used in the transaction
Card Acceptor ID	Code that identifies the card acceptor operating the terminal TCR 1, Positions 81-95
Merchant Name	Name of the merchant TCR 0, Positions 92-116
Terminal ID	Identifies the card acceptor terminal TCR 1, Positions 96-103
Retrieval Reference Number	Transaction reference. For SMS acquirers only SMS: Field 37
Message Type Identifier	Used to identify transaction (for SMS acquirers only) From SMS message header
Processing Code	Used to identify transaction (for SMS acquirers only) SMS: Field 3, Positions 1-2
POS Condition Code	Used to identify transaction (for SMS acquirers only) SMS: Field 25

4 Address Verification Service

Note The service described in this chapter relates to that supported within the Europe region, with some reference to the domestic service available within the United Kingdom (UK). The domestic service available within the USA is not described.

The Address Verification Service (AVS) is used primarily for transactions that take place in a card-absent environment. AVS enables a Merchant to verify a Cardholder's billing address. Based on the results of the verification, a Merchant can make an informed decision regarding whether or not to continue a transaction.

Merchants can submit an address verification request as part of, or separately from, an authorization request.

The service is also used in conjunction with a Card Verification Value 2 (CVV2) check.

4.1 UK domestic service

The UK implementation of AVS was introduced earlier than standard AVS. It can only carry numeric data rather than the full street address.

UK Acquirers forward the numeric data from the Cardholder's street address and post code to UK Issuers for verification and for the results of the verification to be passed back to UK Acquirers.

The Visa Europe Authorization Service (VEAS) converts AVS requests from international locations. UK Issuers may therefore receive requests from outside the UK containing legitimate UK AVS data.

4.2 Related information

For further information about the Address Verification Service, see the following documents:

- *Single Message System (SMS) POS Technical Specifications*
- *Dual Message System Authorization (DMSA) Technical Specifications*
- *Dual Message System Authorization (DMSA) Processing Specifications*
- *UK Card Not Present (CNP) Service Manual*

4.3 Participation

AVS is available through the dual and single messaging systems.

Participation is:

- Mandatory for UK Issuers and Acquirers
 - All Issuers and Acquirers in the UK must support the AVS domestic service and must be certified to receive and to send AVS codes for all products.
- Optional for non-UK Issuers, Acquirers and Merchants

To participate in the service, Members must meet the following requirements.

4.3.1 Testing and certification

Certification is mandatory for Acquirers and Issuers.

AVS certification ensures that the Acquirer can send and receive AVS fields in authorization-related messages, and that the Issuer can receive them and respond with appropriate values in fields:

- 25 - Point-of-Service Condition Code
- 44.2 - Address Verification Result Code
- 123 - Verification Data

For more information, Members should contact Customer Support.

4.3.2 Service monitoring

There is no monitoring for the Address Verification Service.

4.3.3 Planning and implementation

Issuers must ensure their authorization systems can accept and respond appropriately to AVS requests.

4.4 How the service works

For Merchants, AVS provides verification of Cardholder billing addresses; primarily (but not restricted to) card-absent transactions.

Issuers perform the AVS check independently of the authorization decision, which is based on account verification and on the availability of funds. The results of the AVS check are sent to the Acquirer, who in turn, passes on the information to the Merchant. The result of the AVS check assists Merchants in deciding whether to continue with the transaction. As the address check and authorization decision are separate, this could mean that an approval is given by the Issuer, whilst, at the same time, the address check reveals a no match.

To request verification of a Cardholder's address, Merchants submit the verification request as:

- Part of a 0100 authorization request
- Part of a 0200 financial request
- An account verification with AVS data (sent as a 0100 or 0200 message)

To request address verification, Acquirers must include Cardholder billing address and postal code data in field 123 - Verification Data of the message.

VEAS looks at the values in specific message fields to determine:

- Whether the Acquirer requests both address verification and authorization or financial message processing; or
- Whether the Acquirer requests account verification with AVS

Verification request types		
Request type	Field 4	Field 123
Address verification with authorization request	Amount	Address data
Account verification with AVS request	Zeros	Address data

4.4.1 Verification data

The address data that VEAS receives in field 123 contains combinations of the following characteristics:

- Address data standards
- Field formats
- Issuer receipt options

4.4.2 Address verification data standards

The International Data Standard (IDS) for AVS data defines uniform practices for sending address data.

IDS standards for a street address are:

- The address must be only in Extended Binary Coded Decimal Interchange Code (EBCDIC) displayable characters.
- The length can be up to 40 characters. Merchants and Acquirers must have the ability to send a minimum of 20 characters (the number of characters sent can be less than 20).
 - When the Cardholder-provided address exceeds available space, Merchants and Acquirers truncate the right-most characters.
 - When the Cardholder's address is shorter than the available space, Merchants and Acquirers either shorten the field length or space-fill the remainder of the field to the right.
- Acquirers must convert spelt out residence numbers to numerals. For example, Acquirers must send "Thirty-One Park Place" as "31 Park Place".
- Except for converting spelt out residence numbers, Merchants and Acquirers must not perform any other compression or alteration of Cardholder-supplied data.
- Issuers in countries that have fewer than five numeric digits in their postal code should be prepared to receive values of less than five characters, because some Merchants and Acquirers do not send the alpha characters in alphanumeric postal codes.

Non-IDS data must be specifically identified as such within the authorization request. Members that want to establish a data standard that varies from that of the IDS must contact Visa Europe Customer Support.

4.4.3 Data compression

Issuers can choose to receive street address data in either compressed or uncompressed format.

Note In the UK domestic service, compression is mandatory for both street address and post code. The compression algorithm used is unique to the service.

The following compression options are available:

- Leading numerics

The street address subfield is scanned from left to right, and the numeric digits extracted. Scanning stops when a space or an alphabetic character (not including any special characters) is encountered; or when the entire street address has been scanned.

- First five numerics

The street address subfield is scanned from left to right. Scanning stops when five numeric digits are extracted, or when the entire street address has been scanned.

- Post code and first five numerics (UK only)

The post code field is scanned from left to right, and all numerics extracted. The street address subfield is scanned from left to right. Scanning stops when five numeric digits are extracted, or when the entire street address has been scanned.

- Uncompressed

If the Issuer wants to receive street address and postal code data exactly as the Acquirer sent it, VEAS does not perform any compression on the data (including any non-numeric characters).

Examples of the effect of different compression methods are shown in the following table. The circumflex accent character (^) indicates a space. Special characters such as forward slash (/), backward slash (\), hash or number (#) or hyphen (-) are ignored by compression algorithms.

Table 2: Examples of the effect of different data compression methods

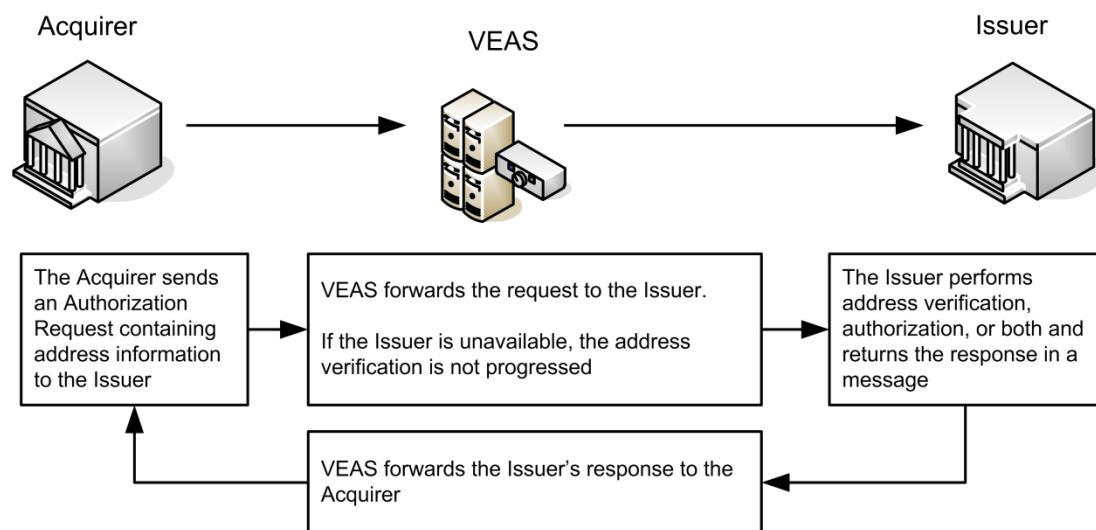
Postal/ZIP code		Street address	Uncompressed	Compressed by leading numerics	Compressed by first five numerics
70433-0123	VE	22 Walnut St #23	704330123 22 Walnut St #23	70433012322	7043301232223
91234-0615	VE	123 1st Street	912340615 123 1st Street	912340615123	9123406151231
91234	VE	2 Elm Street	91234^^^^2 Elm Street	91234^^^^2	91234^^^^^2

Table 2: Examples of the effect of different data compression methods (continued)

Postal/ZIP code		Street address	Uncompressed	Compressed by leading numerics	Compressed by first five numerics
CH48 8AQ	UK	Flat 4a, 147 London Road			488^^^^^4147
B73 6PL	UK	1 Elm Street			736^^^^^1
GU14 7SR	UK	The Ridings, Dean Court			147^^^^^

4.5 Process flows

The following diagram illustrates the process flow for the Address Verification Service.

Figure 4: Process flow for the Address Verification Service

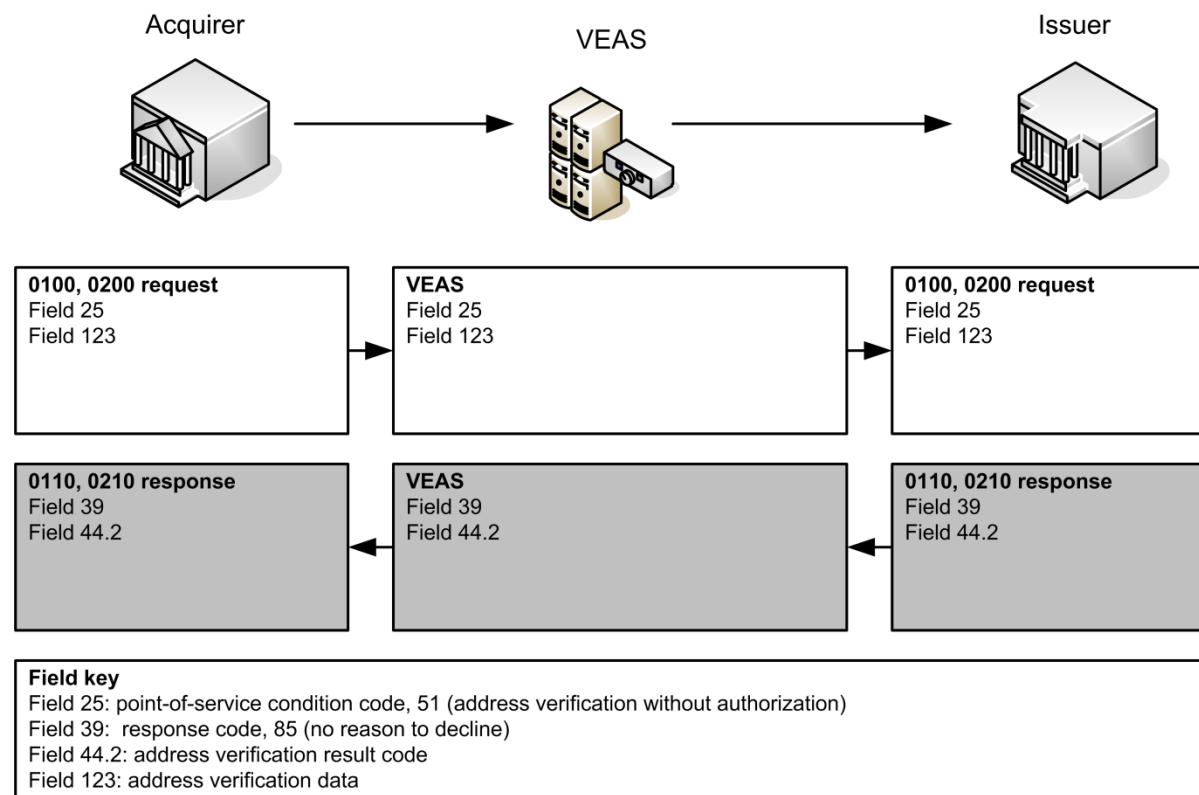
1. The Acquirer submits a 0100 or 0200 authorization request, with address information included, to the Issuer.
2. VEAS receives the request, reformats it in accordance with Issuer options, and forwards it to the Issuer.

If the Issuer is unavailable, VEAS inserts code R (retry) in data field 44.2 - Address Verification Result Code. If the Issuer remains unavailable and the authorization request is routed to STIP, STIP inserts code U (unable to verify).
3. The Issuer inserts the authorization response code in field 39 and the address verification result code in field 44.2, and responds to VEAS.
4. VEAS returns the 0110 or 0210 response to the Acquirer.

4.6 Message flows

The following diagram illustrates the message flow for an account verification with AVS.

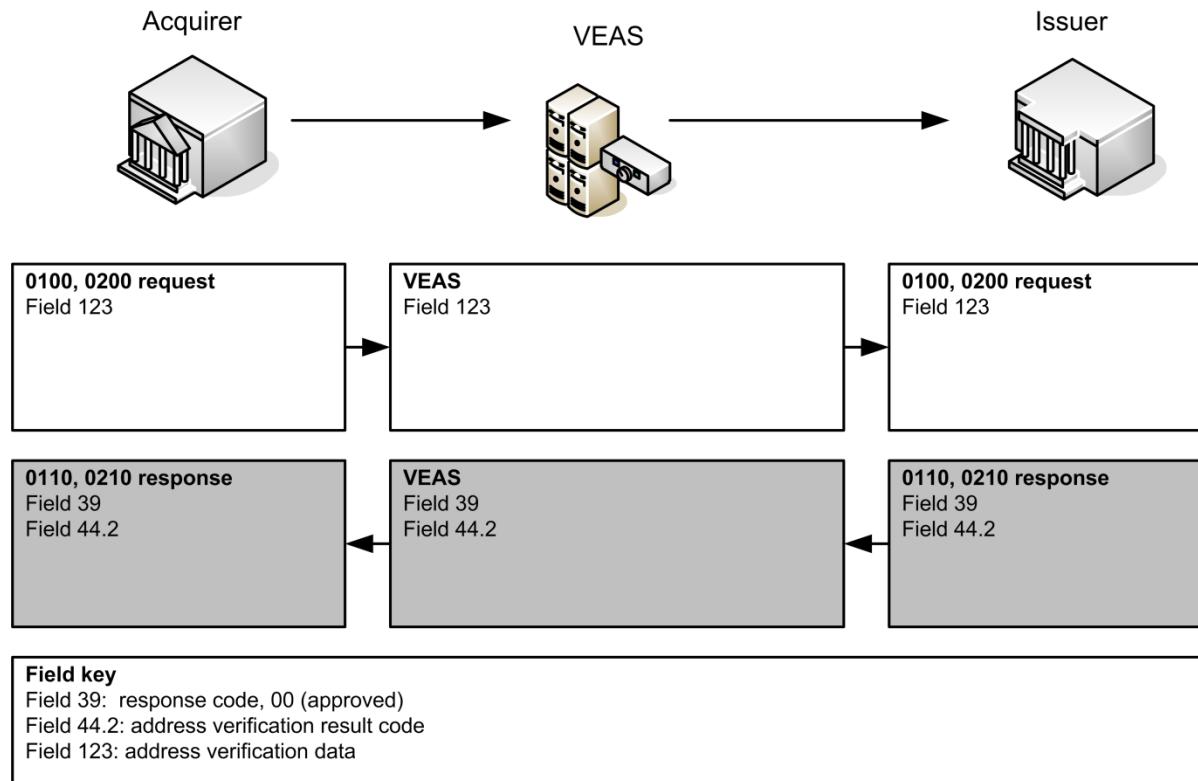
Figure 5: Message flow for the Address Verification Service



1. Acquirer sends a verification request to VEAS.
2. VEAS forwards the request to the Issuer. The address cannot be verified by STIP. However, the account may be verified by STIP if the Issuer is unavailable.
3. Issuer responds to VEAS.
4. VEAS sends response to the Acquirer.

The following diagram illustrates the message flow for a combined authorization and address verification.

Figure 6: Message flow for a combined authorization and address verification



1. Acquirer sends a verification request to VEAS.
2. VEAS forwards the request to the Issuer. STIP is never used to verify an account address. However, the authorization may be processed by STIP if appropriate.
3. Issuer responds to VEAS.
4. VEAS sends response to the Acquirer.

4.7 Key messages

The following messages are relevant to the Address Verification Service:

- 0100 authorization request
- 0110 authorization response
- 0200 financial request
- 0210 financial response

4.8 Key data fields

The following key data fields are used by the Address Verification Service. For detailed information, see the Visa Europe technical specifications.

Data field 3 - Processing Code

This field contains the transaction type and account type (where applicable) affected by the transaction. However, for address verification, this field must be all zeros.

Data field 25 - Point-of-Service Condition Code

This field indicates the transaction conditions at the point-of-service. The code must be set to:

51 - Account verification with AVS only

Data field 44.2 - Address Verification Result Code

This field contains the result of the address verification process. An Issuer uses it only in response to address verification requests.

Data field 123 - Verification Data

This field contains the address details submitted for verification. Issuers can receive the data in the Acquirer's uncompressed or compressed format. For UK domestic transactions, Acquirers use a unique, UK-only compressed format.

5 Advice Retrieval Service - DMSA

The DMSA Advice Retrieval Service enables Issuers to retrieve their advice messages from the DMSA Advice File. The service keeps Issuers informed of stand-in authorizations, reversals and Cardholder Database file updates. An Advice File is created and maintained at each Visa Interchange Center (VIC).

Important VEAS stores DMSA advice records for a maximum of 15 days. After 15 days, VEAS purges any DMSA advice messages that have not been retrieved.

The DMSA Advice File can contain:

- Stand-in processing (STIP) advice messages

Includes authorization requests and reversal requests, the STIP response and the reason why STIP processed the request. STIP does not create advice messages for all the transactions it processes. For example, STIP does not generate advice messages for approved transactions below the advice limit.

- International
- Exception File updates

Notice of Exception File maintenance is initiated by the following services:

- Global Customer Assistance Services (GCAS)
- Automatic Cardholder Database Update (Auto-CDB)

For more information, see *Visa Europe System Management for Members*.

- Automated Fuel Dispenser (AFD) Acquirer Confirmation Advices
Advice messages that confirm the final transaction amount following the completion of the fuel dispense. Acquirer Confirmation Advices are sent in real time without delay to Issuers that have elected to receive them. Otherwise, these messages may be stored in the DMSA advice file depending on Issuer settings and availability.
- Merchant/ATM-initiated advice messages
Real-time advice messages that include ATM dispense adjustments.

Issuers can retrieve advice messages either online or offline.

5.1 Online retrieval

Issuers can retrieve their advice messages online using their Visa Europe System connections. For online retrieval, Issuers must be authorized to access the advice records. Issuers can use either one station or multiple stations to retrieve advice messages.

Online retrieval ensures that Issuers are informed as soon as possible when STIP is involved in a transaction. For example, Issuers may be involved in a situation where a Cardholder's account balance may need to be adjusted.

5.1.1 One station

A single station initiates a sign-on message to retrieve advice messages from the advice queue; one is delivered automatically every two seconds.

5.1.2 Multiple stations

Using multiple stations concurrently allows Processors to retrieve advice messages much more quickly than they can from a single station. Participants may continue advice retrieval from a single station through their primary connection to the Visa Europe System.

5.2 Offline retrieval

Issuers can receive machine-readable or print-ready advice records through the Visa Europe Clearing and Settlement Service (VECSS) as transaction code 48 (TC 48) advice messages. Advice messages are received a day later. Receiving advice messages through VECSS is especially useful when the Issuer is a Processing Centre for both DMSA and VECSS.

Note Visa Europe recommends the use of the online option for advice retrieval (see [Online retrieval](#) on the previous page).

5.3 Related information

For further information about the DMSA Advice Retrieval Service, see the following documents:

- *Visa Europe System Management for Members*
- *Dual Message System Authorization (DMSA) Processing Specifications*
- *Dual Message System Authorization (DMSA) Technical Specifications*

5.4 Participation

The DMSA Advice Retrieval service is available through the dual messaging system. Participation is mandatory for Issuers and Processors that use DMSA. To participate in the service, Members must meet the following requirements.

5.4.1 Testing and certification

Testing and certification are not required.

5.4.2 Service monitoring

Service monitoring is not available for the Advice Retrieval Service.

5.4.3 Planning and implementation

To benefit fully from the DMSA Advice Retrieval Service, Issuers should consider a number of key points.

5.4.3.1 Recovering advice messages

Advice recovery can be configured through a series of Member parameter options. These parameters, maintained by Visa Europe, are as follows:

- Issuers can choose to recover advice messages throughout the day or only during certain periods.
- For each BIN, Issuers can select the method to use to receive advice messages. For example, Issuers can set up some of their BINs for online advice retrieval and other BINs for offline advice retrieval.
- To avoid automatic sign off after recovering the last advice message in the file, Issuers can opt to remain signed on for advice retrieval after the last advice message has been sent. This option is set at the Processing Centre level, and applies to all Issuer host stations assigned to the Processing Centre.

In this set-up, the Issuer host system signs on to advice retrieval mode and downloads all the advice messages in the queue (if any exist). When the last advice message has been received, the station will remain signed on and will do so until the Issuer host sends a sign-off message.

If advice messages are downloaded in batches, it is better that Issuers try to do this outside normal business hours, when Cardholder usage is lower and there is less traffic going through the connection.

For further information, Members should contact Visa Europe Customer Support.

5.4.3.2 Managing online advice recovery

After the end-of-file 0810 message has been received by a station, it is no longer signed on to advice recovery. Issuers should make sure that they sign back on to advice recovery periodically to ensure that advice message queues do not get too large. Many Issuers automate this to avoid busy processing periods. Equally, Issuers should ensure that they are able to control advice retrieval manually.

Some Issuers automate advice retrieval sign on immediately after they have restarted their authorization processing system following maintenance. In most cases this does not cause any issues, but it has been observed that the volume of advice messages in addition to regular authorization traffic can cause the Issuer system to become quickly overburdened. Visa Europe recommends separating the initiation of sign on to advice retrieval from that of regular authorization sign on.

5.4.3.3 Managing Cardholder available balances

Issuers should consider the impact of stand-in processing (STIP) authorization on advice message recovery processing. STIP advice messages reflect authorization decisions that can affect the available funds in a Cardholder's account. If an Issuer restricts advice message recovery to only certain periods, it may find that the Cardholder's credit limit is insufficient to cover the total value of Issuer-approved and STIP-approved transactions.

5.4.3.4 Increased advice message traffic

Issuers must be able to handle increased advice message throughput. Processor host constraints may limit the number of stations that Issuers can sign on to in advice retrieval mode, at one time.

5.4.3.5 Multiple stations

Participants can sign on to multiple stations to speed up advice message recovery. However, before using this option, each Member should analyse their Visa Europe System connection capacity for the following factors:

- Line speed
- Number of stations
- Host connectivity protocol

5.5 How the service works

This section explains how the DMSA Advice Retrieval Service works.

5.5.1 DMSA advice message creation

STIP generates advice messages during authorization and reversal processing. VEAS also generates DMSA advice messages for Exception File updates. For more information about the Exception File, see *Visa Europe System Management for Members*.

Acquirer Confirmation Advice messages are generated by Acquirers. VEAS sends these messages without delay to Issuers that have elected to receive them.

Advice messages are not created for all STIP-processed transactions. For approvals, Issuers can set advice limits, below which transactions do not generate advice messages. See *Positive Cardholder Authorization Service*.

5.5.2 Message processing modes

Participants have the following three modes for message processing:

- Normal mode
- Advice recovery mode
- Advice recovery and normal mode running concurrently

5.5.2.1 Normal mode

Issuers can send and receive request and response messages, but do not receive advice messages.

5.5.2.2 Advice recovery mode

VEAS sends advice messages (stored in the DMSA Advice File) to Issuers. Issuers can choose to sign on for advice recovery from a dedicated station.

See [Process flows](#) below.

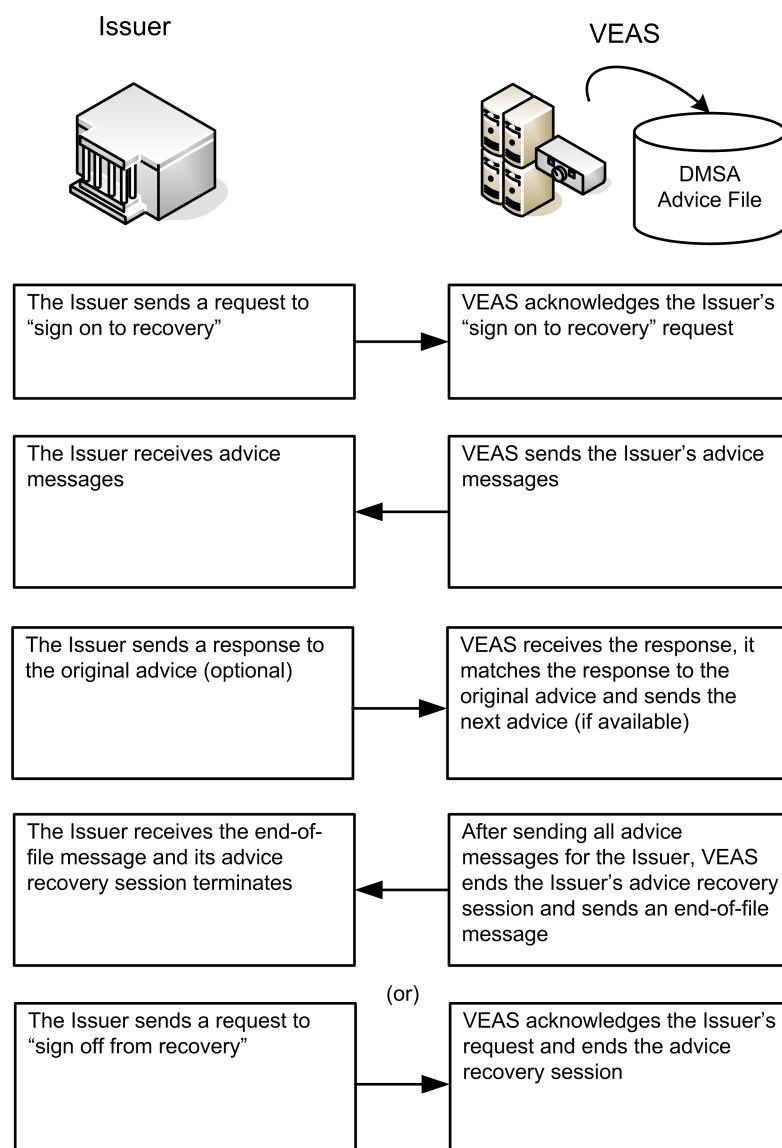
5.5.2.3 Normal and advice recovery mode

Issuers can send and receive real-time authorization messages as well as receive stored advice messages. The Member signs on to recovery while still signed on for normal message processing.

5.6 Process flows

The following diagram illustrates the process flow for the DMSA Advice Retrieval Service.

Figure 7: Process flow for the DMSA Advice Retrieval Service



1. Sign on in advice recovery mode.

To sign on in advice recovery mode and initiate automatic advice message retrieval, an Issuer submits a 0800 message with code 078 in field 70. VEAS acknowledges the request by sending a 0810 response.

If an Issuer chooses to use multiple stations to retrieve advice messages, it must send a separate 'sign on to recovery' message for each participating station. For example, if the Issuer wants to have three stations actively processing advice messages, it must first send three separate 'sign on to recovery' messages.

Priority sequence of VEAS advice messages		
Priority	Message	Description
1	0120	STIP action or Exception File update advice messages
2	0420	Reversal advice messages
3	0620	Administrative advice messages

If a station has concurrent normal and advice recovery modes running, authorization traffic is not interrupted.

2. The Issuer receives advice messages automatically every two seconds per signed on station, without a required response. Issuers can receive advices more frequently, by responding to each advice message. When VEAS receives the response, it matches the response to the original advice and sends the next advice (if available). If the Issuer's response takes longer than two seconds or does not match, then VEAS continues to send advices every two seconds.

Usually, advice messages arrive in chronological order, but creation of advice messages at a secondary Processing Centre may affect the order.

3. Sign off from advice recovery mode.

To sign off from advice recovery, an Issuer sends a 0800 message with code 079 in field 70. VEAS acknowledges the request by sending a 0810 response.

If the Issuer does not send a 0800 request, unless the Issuer requests otherwise, VEAS automatically signs off the Issuer station from advice recovery mode after it delivers the last pending advice message.

- To sign off from an Issuer station, VEAS sends a 0810 network management end-of-file message to the Issuer station, with a value of 079 in field 70
- To resume advice recovery processing at a later time, an Issuer must submit another 'sign on to recovery' message

Issuers can choose to remain in advice recovery mode after recovering all their advice messages from the DMSA Advice File so that they can recover advice messages as VEAS creates them. (See [Recovering advice messages](#) on page 44.)

5.6.1 DMSC advice delivery (offline)

At 00:00 Greenwich Mean Time (GMT) daily, VEAS sends the eligible records from the DMSA Advice File to Dual Message System Clearing (DMSC). DMSC formats the DMSA records as TC 48 advice messages to enable transmission of the advice data through the Interchange Transaction File and on to the DMSC Issuer.

Issuers can select some of their BINs to retrieve advice messages online and can select other BINs to retrieve advice messages offline, through DMSC. However, Issuers cannot set up the same BIN for both the online and offline advice retrieval methods.

DMSC offers two TC 48 record formats for delivering DMSA advice messages: standard and enriched. For information about both formats, see *DMSC Technical Specifications*.

Note The VECSS Advice Retrieval option delays receipt of advice messages until the next processing day.

5.6.2 Advice retrieval during and after a Visa Interchange Center switchover

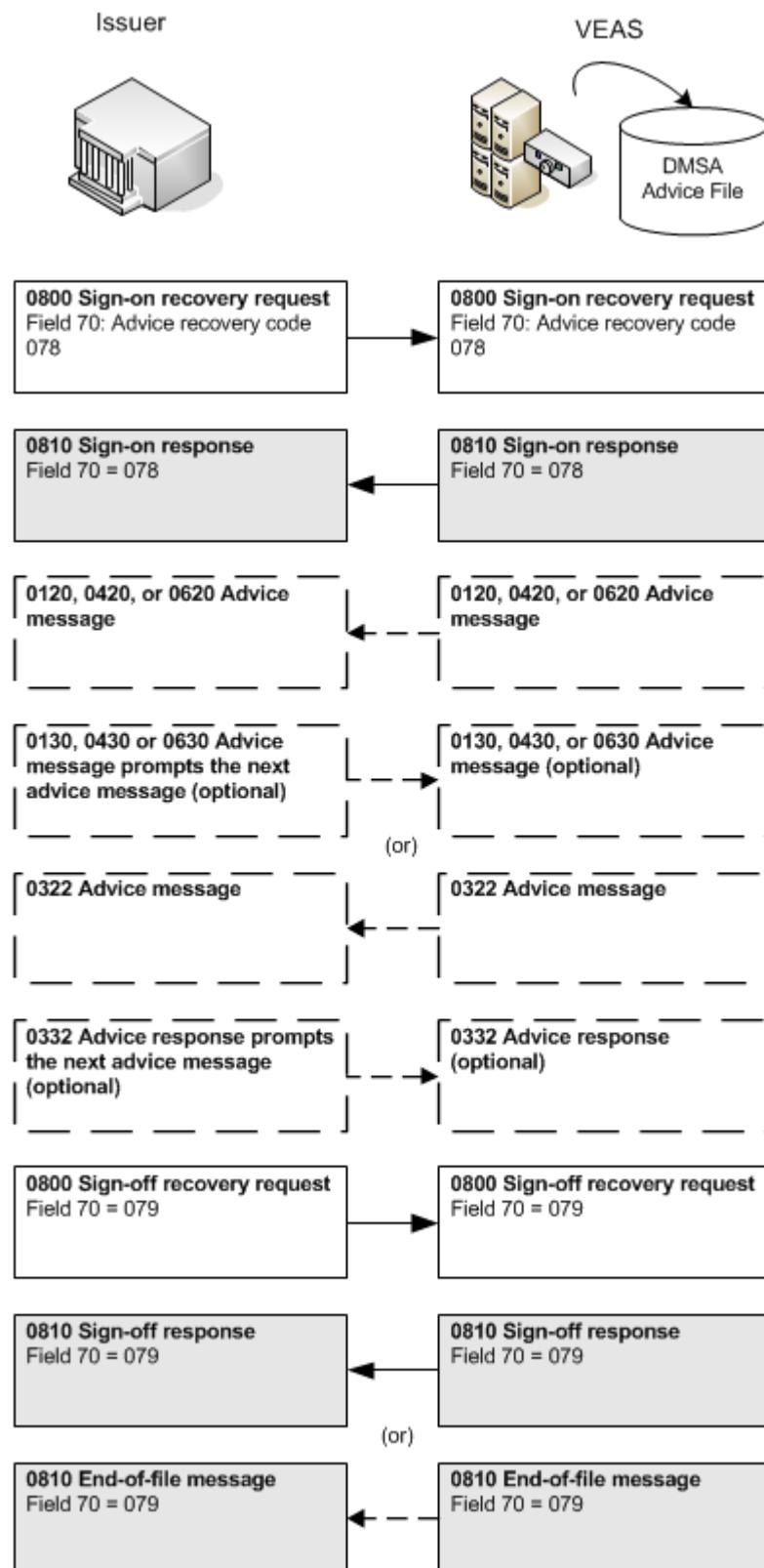
Each Visa Interchange Center maintains its own DMSA Advice File for the responses created by STIP at that centre. Under normal conditions, the file at the Issuer's primary centre contains all transactions processed on the Issuer's behalf. An Issuer usually receives services through its primary centre, but situations may arise that cause the primary centre to switch the Issuer to the secondary centre.

During the switchover, Issuers may receive advice messages out of normal chronological order. However, advice messages will only ever be sent once. No duplicates are produced.

5.7 Message flows

The following diagram illustrates the message flows for the DMSA Advice Retrieval Service.

Figure 8: Message flows for the DMSA Advice Retrieval Service



5.8 Key messages

The following messages relate to the Advice Retrieval Service:

- 0120 advice message

This advice message may be:

- A notice of a request and its response data when STIP processes a balance inquiry, authorization request or an address verification-only request on behalf of a dual message Issuer.
- A VEAS generated DMSA Exception File update advice message for updates made by the Automatic Cardholder Database Update (Auto CDB) Service, and the Global Customer Assistance Service (GCAS).
- An Acquirer Confirmation Advice

Issuers using DMSA can receive these advice messages as 0120 messages, or as Dual Message System Clearing (DMSC) TC 48 advice messages.

- 0130 advice response (optional)

To receive advices faster, Issuers respond to the original 0120 advice message, by sending a 0130 advice response. This prompts VEAS to send the next advice message in the DMSA Advice file.

- 0322 file maintenance advice message

This advice message indicates that VEAS updated the Cardholder Database on the Issuer's behalf. Dual message Issuers can choose to receive either 0120 or 0322 file update advice messages, but not both.

If a dual message Issuer chooses to receive 0322 file update advice messages, it may optionally send 0332 advice response messages.

- 0332 file maintenance advice response (optional)

To receive advices faster, Issuers respond to the original 0322 file maintenance advice message by sending a 0332 file maintenance response. This prompts VEAS to send the next advice message in the DMSA Advice file.

- 0420 reversal advice message

This advice message notifies the Issuer when STIP processes a 0400 reversal and advice message creation is appropriate under the rules of the Positive Cardholder Authorization Service (PCAS).

- 0430 reversal advice response (optional)

To receive advices faster, Issuers respond to the original 0420 reversal advice message, by sending a 0430 reversal advice response. This prompts VEAS to send the next advice message in the DMSA Advice file.

- 0620 administrative advice message

Free text administrative advice messages communicate information on chip-based transactions, including authentication failures and Issuer script advice messages.

- 0630 administrative advice response (optional)

To receive advices faster, Issuers respond to the original 0620 administrative advice message, by sending a 0630 administrative advice response. This prompts VEAS to send the next advice message in the DMSA Advice file.

- 0800 network management request

This message allows Issuers to sign on to advice recovery mode. Issuers use code 078 to sign on to recover advice messages automatically, and code 079 to stop the recovery process.

- 0810 network management response

This message allows Issuers to sign off from advice recovery mode. VEAS also uses a 0810 message to send an end-of-file notification to the Issuer, indicating that the Advice File contains no more advice messages to recover.

5.9 Key data fields

The following key data field is used by the Advice Retrieval Service. For detailed information, see the Visa Europe technical specifications.

Data field 70 - Network Management Information Code

This field contains a code that defines the type of network management needed:

- Network sign-on or sign-off
- Start or stop transmitting advice messages
- Communications link test between a Processing Centre and the user

6 Advice Retrieval Service - SMS

This section provides a brief description of the Single Message System (SMS) Advice Retrieval Service and explains which Members are eligible for this service.

The SMS Advice Retrieval Service enables Acquirers and Issuers to use online connections to recover all types of advice messages from the SMS Advice File. The service allows Members to decide when they want to retrieve advice messages so they can manage their advice message volume efficiently. An Advice File is created and maintained at each Visa Interchange Center.

The SMS Advice File includes the following:

- Stand-In Processing (STIP) processing advice messages
 - Includes STIP authorization responses, reversal response records, the STIP response, and the reason why STIP processed the request.
- Deferred clearing advice messages (including Automated Fuel Dispenser confirmations)
- SMS reversal and exception item processing advice messages (including chargebacks initiated by Issuers)
- SMS file maintenance advice messages
- SMS reconciliation totals advice messages
- Funds transfer totals messages
- Fraud reporting advice messages

Important VEAS stores SMS advice messages online for 30 days. Issuers and Acquirers that use SMS and want to retrieve their advice messages need to retrieve them within this 30-day period. After 30 days, SMS advice messages are written to an archive, and deleted from the VEAS Advice File. Members wishing to recover such archived advice messages must contact Visa Europe Customer Support.

Issuers and Acquirers retrieve advice messages online.

6.1 Online retrieval

Service participants retrieve their advice data online through their Visa Europe System connections. Participants can use either one station or multiple stations to retrieve advice messages.

6.1.1 One station

A single station initiates a sign-on message to retrieve advice messages from the advice queue. Each successfully retrieved advice message (xx20) must be acknowledged (xx30). After an advice message is acknowledged, the next advice message in the queue is sent.

6.1.2 Multiple stations

Using multiple stations concurrently allows Processors to retrieve advice messages much more quickly than they can from a single station. Participants may continue advice retrieval from a single station through their primary connection to the Visa Europe System.

6.2 Related information

For further information about the Advice Retrieval Service, see the following documents:

- *Single Message System (SMS) ATM Processing Specifications*
- *Single Message System (SMS) ATM Technical Specifications*
- *Single Message System (SMS) POS Processing Specifications*
- *Single Message System (SMS) POS Technical Specifications*
- *Visa Europe System Management for Members*

6.3 Participation

The SMS Advice Retrieval Service is available through the single messaging system. Participation is mandatory for Issuers, Acquirers and Processors that use SMS. To participate in the service, Members must meet the following requirements.

6.3.1 Testing and certification

Testing and certification are not required.

6.3.2 Service monitoring

Service monitoring is not available for the Advice Retrieval Service.

6.3.3 Planning and implementation

To benefit fully from the SMS Advice Retrieval Service, Members should consider a number of key points.

6.3.3.1 Recovering advice messages

Participants can choose to recover advice messages throughout the day or only during certain periods.

6.3.3.2 Managing online advice recovery

Issuers that are in the habit of signing off from advice retrieval should ensure that they sign back on to advice recovery periodically to ensure that advice queues do not get too large. Many Issuers automate this in their systems to avoid busy processing periods. Equally, Issuers should ensure that they are able to control advice retrieval manually.

Some Issuers automate advice retrieval sign on immediately after they have restarted their authorization processing system following maintenance. Whilst in most cases this does not cause any issues, it has been observed that the volume of advice messages in addition to regular authorization traffic can cause the Issuer system to become quickly overburdened. Visa Europe recommends separating the initiation of sign on to advice retrieval from that of regular authorization sign on.

6.3.3.3 Managing Cardholder available balances

Issuers should consider the impact of Stand-In Processing (STIP) authorization on advice message recovery processing. STIP advice messages reflect authorization decisions that can affect the available funds in a Cardholder's account. If an Issuer restricts advice message recovery to only certain periods, it may find that the Cardholder's credit limit is insufficient to cover the total value of Issuer-approved and STIP-approved transactions.

6.3.3.4 Increased advice message traffic

Issuers must be able to handle increased advice message throughput. Processor host constraints may limit the number of stations that Issuers can sign on to advice retrieval mode at one time.

6.3.3.5 Same station for advice retrieval and response

The Visa Europe System must receive a response from the same station that originated the request. Processors must ensure that the station that sends the original advice request sends the advice response back to the Visa Europe System.

6.3.3.6 Multiple stations

Participants can sign on to multiple stations to speed up advice message recovery. However, each Member should analyse their Visa Europe System connection capacity for the following factors before using this option:

- Line speed
- Number of stations
- Host connectivity protocol

6.4 How the service works

This section explains how the SMS Advice Retrieval Service works.

6.4.1 SMS advice message creation

Acquirers, Issuers, SMS STIP or SMS itself can create advice messages. VEAS stores all incoming DMSC transactions as advice messages at the end of the offline clearing process. These transactions can include financial and representment requests. VEAS also stores all system-generated reversals as advice messages.

Acquirers use advice messages to deliver or to represent financial transactions to Issuers for settlement and for account posting. In general, Acquirers generate an advice message when a transaction does not require authorization processing either by the Issuer or by STIP, such as a representment. Subject to programme operating rules, Acquirers may also use an advice message instead of a request if they are unable to send the request in real-time because of communication problems.

Issuers use advice messages to chargeback financial transactions or to initiate fee-related transactions.

STIP uses advice messages to notify Issuers of authorization and financial transactions processed under stand-in conditions. An advice message contains the request and the STIP response. It provides the information the Issuer needs for account maintenance and for settlement of financial transactions.

SMS uses advice messages when supplying Members with undeliverable approval responses, settlement information, and status advice messages.

VEAS also uses advice messages for updating the SMS Exception File. For information about the Exception File, see the *Visa Europe System Management for Members* document.

6.4.1.1 VEAS advice messages

VEAS also creates SMS advice messages for the advice queue when:

- The Acquirer host does not respond or is unable to respond to an incoming message
- The back-office message originates from a dual message Processing Endpoint

6.4.1.2 Deferred clearing advice messages

A deferred clearing advice message is the result of a transaction between a dual message Acquirer and an SMS Issuer. When the completed transaction is cleared in DMSC, bridging between Visa systems ensures that the SMS Issuer receives a deferred clearing advice message (0220). Acquirers may submit deferred clearing advice messages several days after authorization. The following table lists the elements that identify deferred clearing advice messages.

Table 3: Deferred clearing advice messages

Field	Name	Value	Description
Header field			
10	Batch number	255	Visa Europe System assigned batch number. Batch number '255' is assigned to all advice messages created for transactions coming from DMSC Processing Endpoints
Message field			
63.3	Message reason code	2105	Acquirer generated advice message: clearing of an authorized transaction

Table 3: Deferred clearing advice messages (continued)

Field	Name	Value	Description
63.4	STIP/switch reason code	9100 9101	DMSC advice message: transaction or message received through the DMSC system from a DMSA Processing Centre

6.4.2 Message processing modes

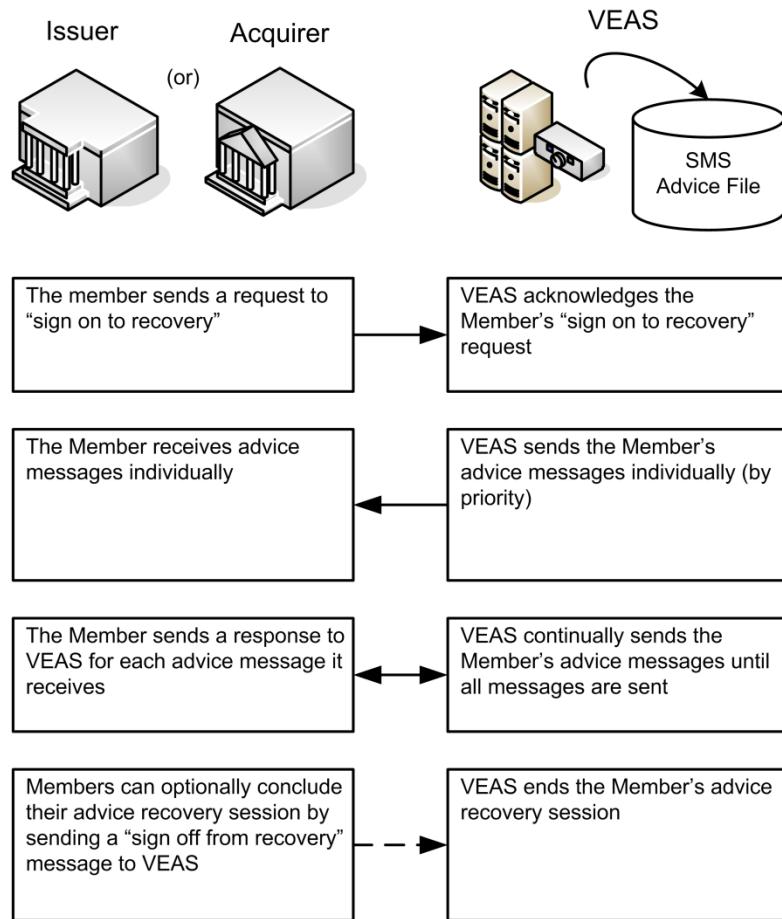
Participants have the following three modes for message processing:

- Normal mode
Issuers can send and receive request and response messages, but do not receive advice messages.
- Advice recovery mode
VEAS sends advice messages (stored in the SMS Advice File) to Members.
- Advice recovery and normal mode running concurrently
Members can send and receive real time messages as well as receive stored advice messages. The Member 'signs on to recovery' while still signed on for normal message processing.

6.5 Process flows

The following diagram illustrates the process flow for the SMS Advice Retrieval Service.

Figure 9: Process flow for the SMS Advice Retrieval Service



1. Sign on in advice recovery mode.

To sign on in advice recovery mode and initiate advice retrieval, a Member submits a 0800 message with code 078 (recommended) or 088 in field 70. VEAS acknowledges the request by sending a 0810 response.

If a Member chooses to use multiple stations to retrieve advice messages, it must send a separate 'sign on to recovery' message for each participating station. For example, if the Member wants to have three stations actively processing advice messages, it must first send three separate 'sign on to recovery' messages. The Member must still respond to each advice message individually before retrieving the next message from the advice queue.

VEAS sends advice messages to the Member station in the following priority sequence.

Priority sequence of VEAS advice messages		
Priority	Message	Description
1	0220	Financial advice messages
2	0420	Reversal advice messages

Priority sequence of VEAS advice messages		
Priority	Message	Description
3	0520	Reconciliation advice messages
4	0620	Administrative advice messages
5	0220	DMSC deferred clearing advice messages

If a station has concurrent normal and advice recovery modes running, authorization traffic is not interrupted.

2. Sign off from advice recovery mode.

Stations signed on to advice recovery mode are expected to remain signed on permanently. Automatic sign-off is not performed after recovery of the last advice message in the file.

If sign off is required, then a Member sends a 0800 message with either code 079 (recommended) or 089 in field 70. VEAS acknowledges the request by sending a 0810 response.

6.5.1 Advice retrieval during and after a Visa Interchange Center switchover

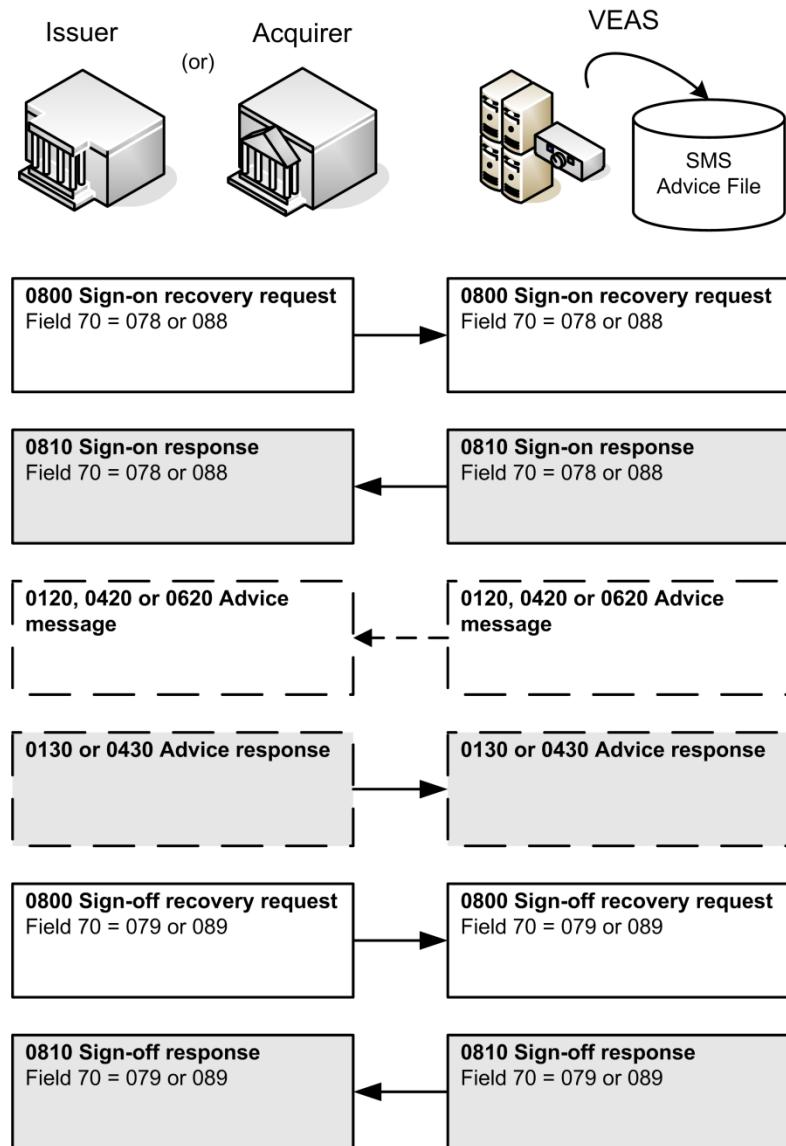
Each Visa Interchange Center maintains its own SMS Advice File for the responses created by STIP at that centre. Under normal conditions, the file at the Member's primary centre contains all transactions processed on the Member's behalf. A Member usually receives services through its primary centre, but situations may arise that cause the primary centre to switch the Member to the secondary centre.

During the switchover, advice messages are stored in the Advice File at the secondary Visa Interchange Center. Issuers that choose to recover advice messages during the switchover should be aware that some advice messages may still be on file at the primary centre. Issuers cannot recover these advice messages until the Visa Europe System switches them back to their primary centre.

6.6 Message flows

The following diagram illustrates the message flows for the SMS Advice Retrieval Service.

Figure 10: Message flows for the SMS Advice Retrieval Service



6.7 Key messages

The following messages relate to the Advice Retrieval Service:

- 0220 STIP processing advice message

This advice message notifies an Issuer that STIP acted on its behalf and processed a 0200 financial transaction (original or adjustment); or it responded to a 0200 balance inquiry, account transfer, representment or merchandise credit. SMS STIP creates the advice message for the Issuer and stores it in the Advice File for the Issuer to recover. The Issuer must respond with a 0230 advice response.

- 0220 advice message of a dual message transaction (deferred clearing advice)
This advice message notifies an SMS Issuer that DMSC processed a financial transaction from a dual message Acquirer. SMS generates the advice message on receipt of the transaction from DMSC and stores it in the Advice File for the Issuer to recover. The Issuer must respond with a 0230 advice response.
- 0220 representation request
An SMS Acquirer uses a 0220 message to submit a representation.
- 0230 financial transaction advice response
This message acknowledges receipt of a 0220 advice message.
- 0322 file maintenance advice message
This advice notifies an Issuer that VEAS updated the Cardholder database file on the Issuer's behalf; the advice includes the updated record content.
- 0332 file maintenance advice response
SMS Issuers must send this response message to acknowledge receipt of a 0322 file maintenance advice. (Dual message Issuers that choose to receive 0322 file maintenance advices may optionally acknowledge their receipt with these response messages.)
- 0420 reversal advice message
The Issuer receives this advice when STIP processes a 0400 reversal on behalf of the Issuer. The Issuer must respond with a 0430 advice.
- 0430 reversal advice response
This message acknowledges receipt of a 0420 reversal advice message.
- 0422 chargeback advice message
This advice message is used for chargeback reversals, Issuer fee collection or funds disbursement, and notification of DMSC transactions. This advice message requires a 0432 advice response.
- 0432 chargeback advice response
This message acknowledges receipt of a chargeback, chargeback reversal, or Issuer-initiated fee collection or funds disbursement.
- 0520 reconciliation totals advice message
This message is an advice that conveys gross Interchange totals (the transaction totals SMS accumulated exclusive of transaction fees and charges and any DMSC deferred clearing items) to an Acquirer or to an Issuer.
- 0530 reconciliation totals advice response
This advice is the response to a 0520 reconciliation advice message. This reply indicates that the Member agrees or disagrees with SMS totals, or alternatively, that the Member is simply acknowledging receipt of the totals.
- 0620 administrative advice message
Includes funds transfer advice messages and Issuer script update advice messages.

- 0630 administrative advice response

This message is the response to a 0620 administrative advice message. The response code from an SMS centre must be 00.

6.8 Key data fields

The following key data fields are used by the Advice Retrieval Service. For detailed information, see the Visa Europe technical specifications.

Header field 9 - Message Status Flags

This header field determines how a message is processed. It contains advice-related flags set by the Visa Europe System which the Issuer or Acquirer can examine during incoming message processing.

Data field 63.4 - STIP/Switch Reason Code

This field indicates the reason why SMS STIP responded on behalf of the Issuer, or why SMS generated an advice message. 0120, 0220, and 0420 advice messages and all incoming DMSC transactions contain this field.

Data field 70 - Network Management Information Code

This field contains a code that defines which one of the following types of network management is needed:

- Network sign-on or sign-off
- Start or stop transmitting advice messages
- Communications link test between a Processing Centre and the user

7 ATM/POS Split Routing Service

The ATM/POS Split Routing Service enables Members to route transactions to different Processing Centres according to the transaction type. The service offers the following options:

- ATM/POS Split Routing
 - Enables Issuers to separate ATM transactions from POS transactions and to route these transactions to different Processing Centres.
 - An ATM transaction has a Merchant Category Code (MCC) of 6011 in the authorization request. Any transaction that contains a different MCC in the request is routed as a POS transaction.
- ATM Account-Type Split Routing
 - Enables Issuers to route ATM transactions according to selected account types when a Cardholder uses a multi-purpose card.
- Alternate Routing
 - Enables Members that use SMS to use one or two secondary Processing Centres to process exception and other back-office transactions.

7.1 Related information

For further information about the ATM/POS Split Routing Service, see the following documents:

- *Introducing the Visa Europe System*
- *Introducing the Visa Europe Authorization Service*
- *Introducing Single Message System (SMS) and Dual Message System Authorization (DMSA) Transactions*
- *Introducing Single Message System (SMS) and Dual Message System Authorization (DMSA) Messages*
- *Dual Message System Authorization (DMSA) Technical Specifications*
- *Visa Europe Merchant Data Standards Manual*

7.2 Participation

The ATM/POS Split Routing Service is available through the dual and single messaging systems.

Participation is optional for Members and subject to the following conditions:

- ATM/POS Split Routing supports Visa, Visa Electron, V PAY and Plus ATM and is available only to Issuers
- ATM Account-Type Split Routing supports Visa ATM and Plus ATM and is available only to Issuers

- Alternate Routing for exception and back-office transactions supports Visa, Visa Electron, V PAY and Plus ATM and is available only to Members that use SMS

ATM/POS Split Routing options may be incompatible with PIN/No-PIN Split Routing options. Members must ensure that they understand their particular configurations and should contact Visa Europe Customer Support to discuss participation.

To participate in the service, Members must meet the following requirements.

7.2.1 Testing and certification

While participating Members do not have to be certified for the ATM/POS Split Routing Service, Members must be certified to send and to receive ATM and POS transactions. To arrange for testing and certification, contact Visa Europe Customer Support.

7.2.2 Planning and implementation

To fully benefit from the service and to better understand available routing parameters, contact Visa Europe Customer Support.

7.3 How the service works

The following sections describe how the service options work.

7.3.1 ATM/POS Split Routing

ATM/POS Split Routing enables Issuers that process Visa, Visa Electron, V PAY and Plus transactions to use separate Processing Centres for ATM and POS transactions. VEAS routes incoming ATM transaction requests to the Issuer's primary Processing Centre and routes POS transaction requests to the Issuer's secondary Processing Centre.

7.3.2 ATM Account-Type Split Routing

VEAS routes transactions based on the account that the Cardholder selects when using a multi-purpose card at an ATM. Issuers can specify up to three Processing Centres: one for deposit accounts, one for credit accounts, and one for universal and non-specified accounts.

7.3.3 Alternate Routing

VEAS allows Members that use SMS to designate secondary Processing Centres for their back-office and exception transactions. Members can also specify separate secondary Processing Centres for their ATM and POS exception transactions.

Designated secondary Processing Centres can send and receive back-office and exception transactions.

An Acquirer that participates in the service can send all original transactions to VEAS through their primary Processing Centre and send all exception and back-office transactions through their secondary Processing Centre.

If the Issuer participates in the service, VEAS can route ATM and POS transactions to one Processing Centre, and back-office and exception transactions to another Processing Centre.

The secondary Processing Centres can be connected to the SMS component of VEAS or to an exception processing system such as Visa Exceptions or the Electronic Documentation Transfer Method.

This option enables Issuers that use SMS to receive back-office items from Acquirers connected either to DMSA or SMS components of VEAS or VECSS.

Alternate routing can apply to:

- Members that use Processors for back-office items at secondary sites
- Members that want to consolidate back-office processing by product
- Members attached both to SMS and to VECSS
- Members that use separate systems for ATM and POS transaction processing

Note Irrespective of the configuration of a Member that uses SMS, they can always initiate back-office or exception items through their regular Processing Endpoint for clearing (VECSS). However, to receive such transactions through their Processing Endpoint for clearing, the Member must specify VECSS as the alternate Processing Endpoint.

7.4 Process flows

The following sections describe the process flows for each of the available service options.

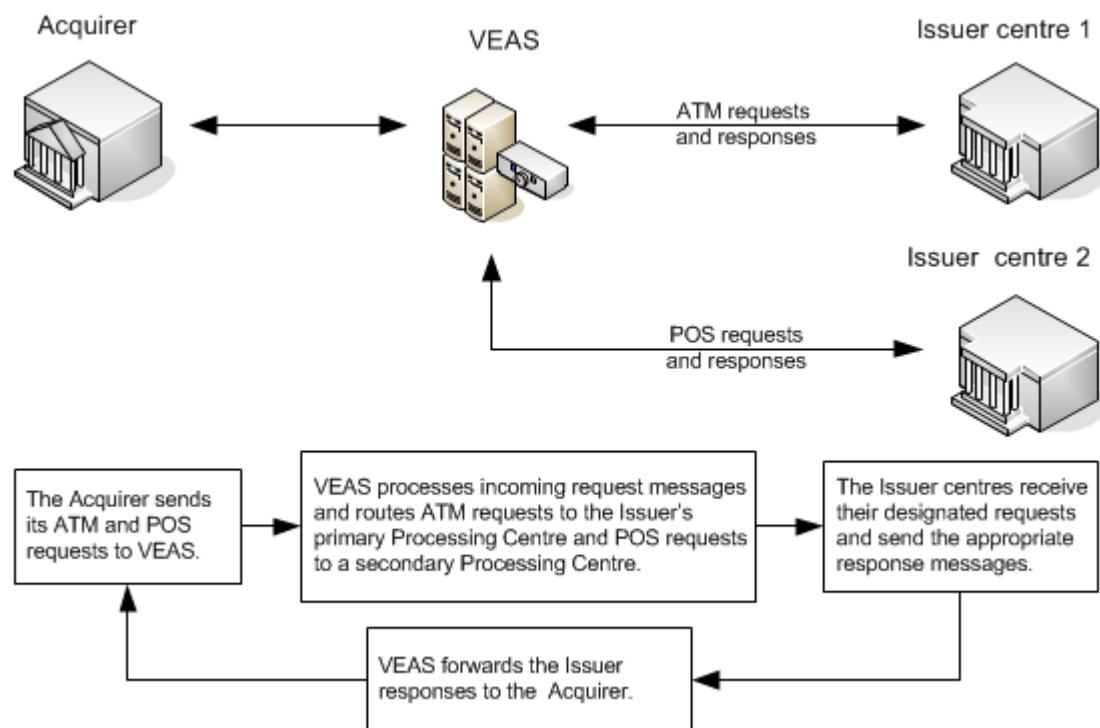
7.4.1 ATM/POS Split Routing process flow

The main steps in ATM/POS Split Routing are:

1. The Acquirer sends transaction requests to VEAS.
2. VEAS routes ATM requests and POS requests to separate Issuer designated Processing Centres.
3. The Issuer's Processing Centres process the requests and return the appropriate responses to VEAS.
4. VEAS forwards the responses to the Acquirer.

The following diagram illustrates the process flow for an Issuer that has a primary Processing Centre designated for ATM transactions and a secondary Processing Centre designated for POS transactions.

Figure 11: Process flow for ATM/POS Split Routing



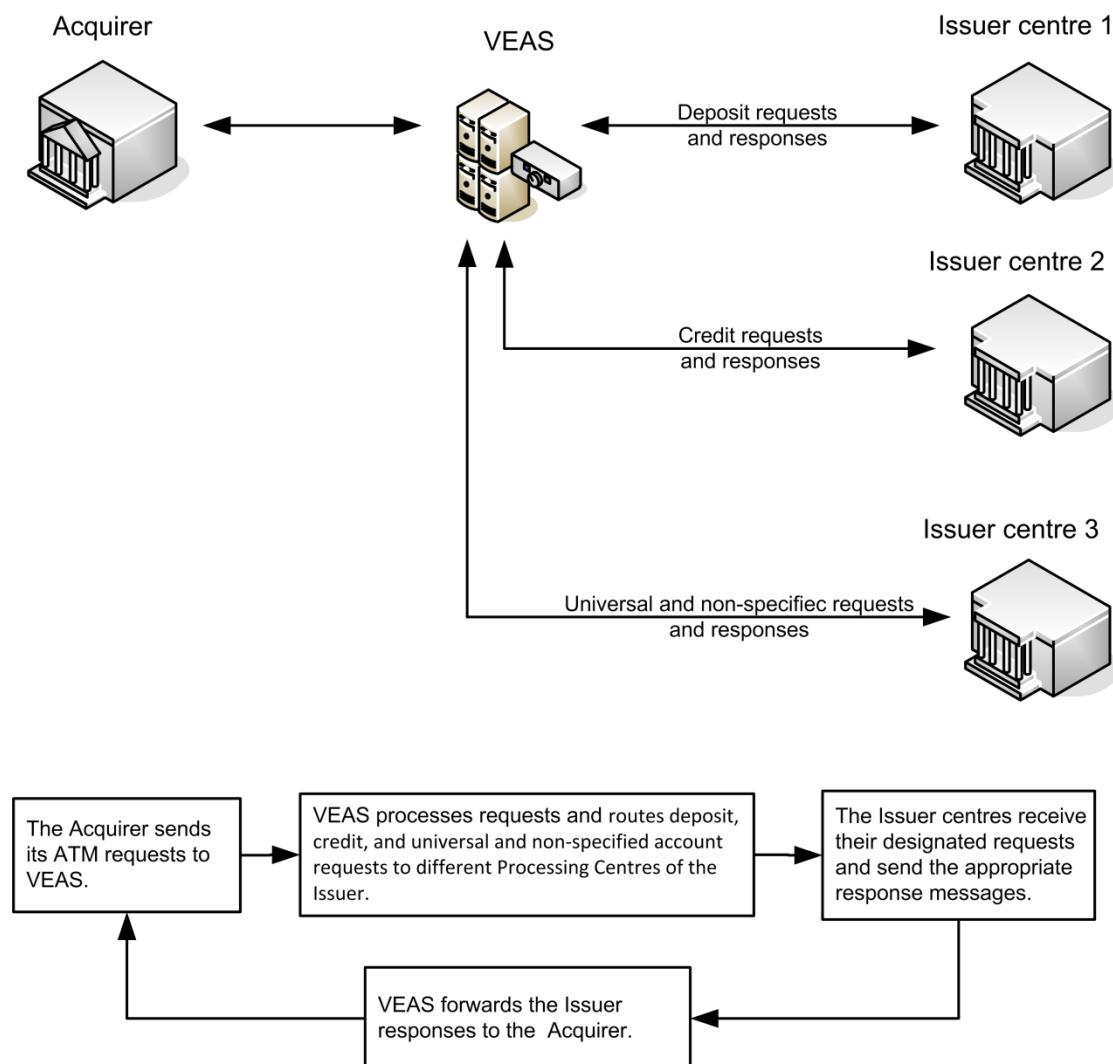
7.4.2 ATM Account-Type Split Routing process flow

The main steps in the ATM Account-Type Split Routing are:

1. At the ATM, the Cardholder selects the account type for the transaction.
2. The Acquirer sends transaction requests to VEAS.
3. VEAS routes requests determined by the account type with which the transaction is associated. For example, an Issuer can use up to three different Processing Centres for deposit, credit, and universal/non-specified accounts.
4. The Issuer's Processing Centres process the requests and return the appropriate responses to VEAS.
5. VEAS forwards the responses to the Acquirer.

The following diagram illustrates the process flow for an Issuer that has separate Processing Centres for deposit requests, credit requests, and universal and non-specific requests.

Figure 12: Process flow for ATM Account-Type Split Routing



7.4.3 Alternate Routing option process flow

The main steps in the Alternate Routing option are:

1. If an Acquirer participates in the Alternate Routing option, the Acquirer's primary Processing Centre sends all original ATM and POS transactions requests to VEAS. The Acquirer's secondary processing centre may send some or all exception and back-office requests to VEAS.

Note The Acquirer's secondary Processing Centre will receive any exception items, for example, chargebacks.

2. VEAS performs the following functions according to the Issuer's Alternate Routing configuration:

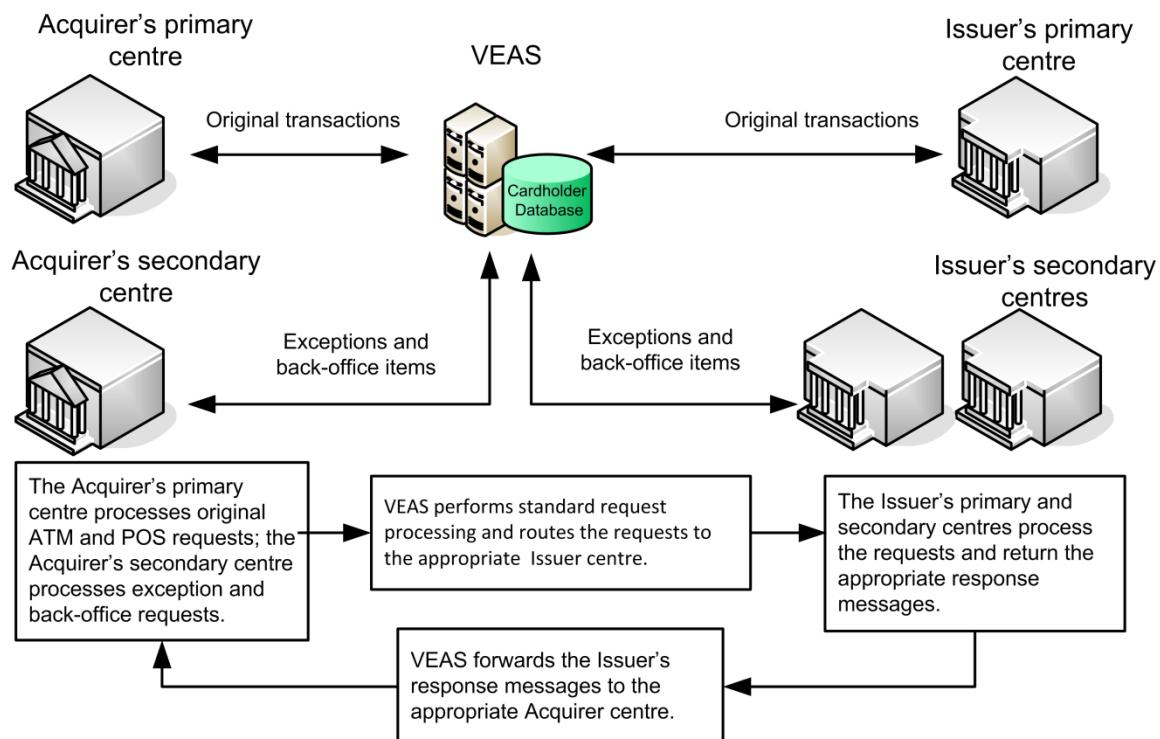
- Routes all original ATM and POS transaction requests to the Issuer's primary Processing Centre
- Routes all exception, administrative and other back-office (non-original) requests to the Issuer's secondary Processing Centre

Note If the Issuer has two secondary Processing Centres, VEAS routes all non-original ATM requests to one secondary Processing Centre, and all non-original POS requests to the other secondary Processing Centre.

3. The Issuer's Processing Centres process the requests and return the appropriate responses to VEAS.
4. VEAS routes the responses to the Acquirer's primary and secondary Processing Centres, as appropriate.

The following diagram illustrates the process flow for an Acquirer that has one secondary Processing Centre and an Issuer that has two secondary Processing Centres. In this scenario, the Acquirer's primary Processing Centre submits original ATM and POS transactions and the Acquirer's secondary Processing Centre submits exception and back-office items.

For the Issuer, VEAS routes all original transactions to the Issuer's primary Processing Centre, all non-original ATM transactions to one of the Issuer's secondary Processing Centres, and all non-original POS transactions to the Issuer's other secondary Processing Centre.

Figure 13: Process flow for Alternate Routing option

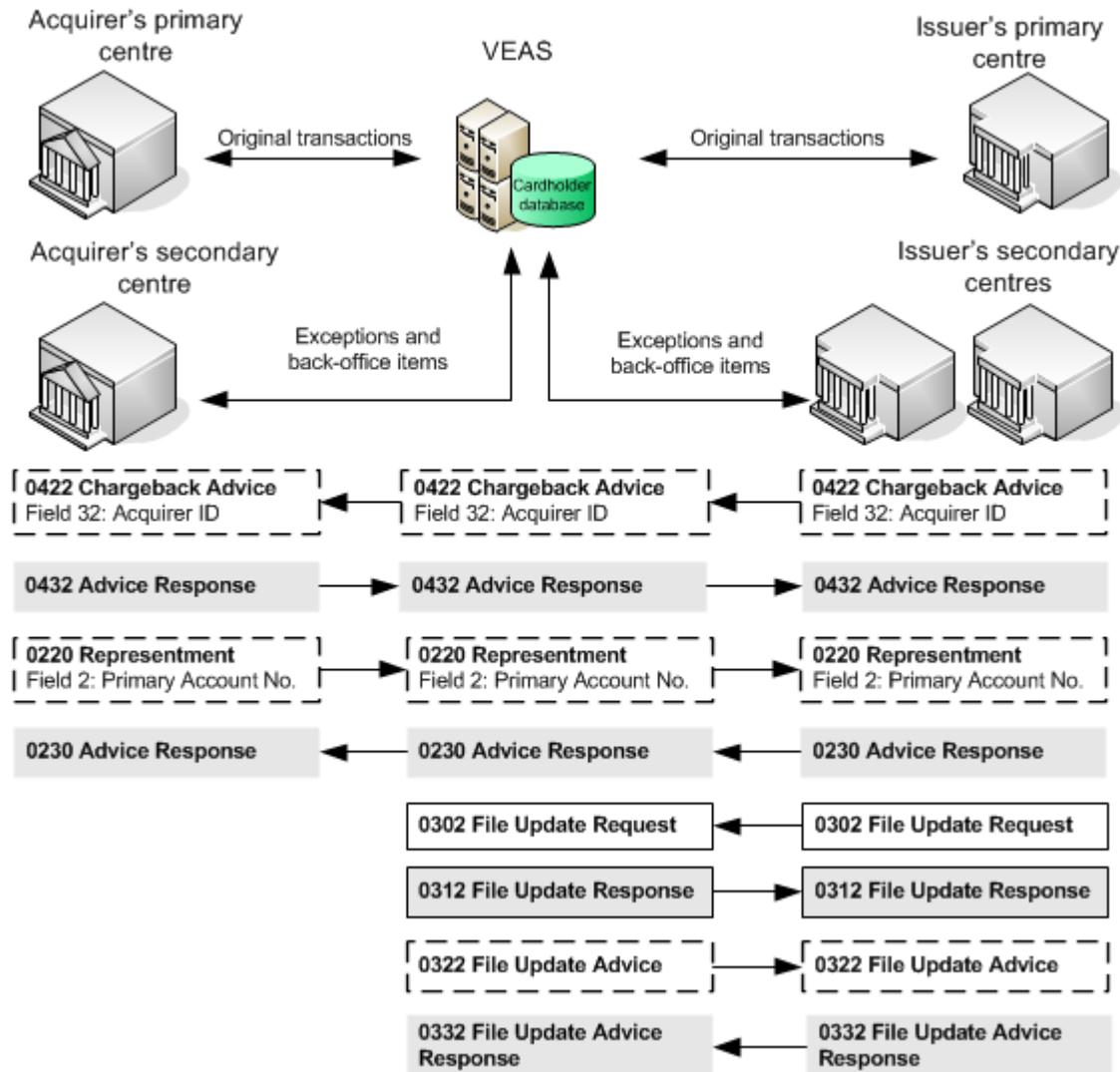
Members can also use secondary Processing Centres for settlement processing. The Visa Europe System settles transactions routed to a secondary Processing Centre according to the settlement attributes specified for the primary Issuer or Acquirer unless the Processing Centre specifies alternative settlement.

7.5 Message flows

ATM/POS Split Routing and the ATM Account-Type Split Routing do not alter the standard message flows as described in the *Introducing SMS and DMSA Transactions* manual. VEAS routes messages according to the key data field values identified in [Key data fields](#) below.

The following diagram illustrates the message flow for Alternate Routing.

Figure 14: Message flow for the Alternate Routing



7.6 Key data fields

The following key data fields are used by the ATM/POS Split Routing Service. For detailed information, see the Visa Europe technical specifications.

Data field 2 - Primary Account Number

Service options: ATM/POS Split Routing, ATM Account-Type, Alternate Routing

This data field contains the account number that is used to determine the routing. Data field 2 is used in 0100/0110 and 0200/0210 requests and responses for all split routing options.

Data field 3 - Processing Code (positions 1 and 2)

Service options: Alternate Routing

Positions 1 and 2 in this data field contain a value that identifies the transaction type. For the Alternate Routing option, this value helps to indicate (along with the message type) whether the request is a purchase or an exception transaction.

Data field 3 - Processing Code (positions 3 and 4)

Service options: ATM Account-Type

Positions 3 and 4 in this data field contain a value that identifies the account types, if any, specified in the request. VEAS routes the requests according to the account type. Up to three Processing Endpoints can be specified.

Data field 18 - Merchant Type

Service options: ATM/POS Split Routing, ATM Account-Type, Alternate Routing

This data field contains a value that identifies the Merchant type associated with the request. This data field is used in all requests and advice messages that relate to a transaction or to an electronic banking payment. For ATM-only transactions, the Merchant Category Code must be 6011 for all original 0100 and 0200 requests and associated exception item messages.

Subfield 63.1 - Network Identification Code

Service options: ATM/POS Split Routing, ATM Account-Type, Alternate Routing

This data field contains a value that identifies the network that VEAS uses to transmit the message.

Subfield 63.3 - Message Reason Code

Service option: Alternate Routing

This data field contains a value that identifies the reason for generating the message.

8 Authorization Gateway Services

The Visa Europe Authorization Service (VEAS) is responsible for routing messages to the correct destinations. If the destination of a transaction is a system or a network outside the Visa Europe System (or outside Visa Inc.'s authorization service), Authorization Gateway Services enable acquirers to route non-Visa transactions through the Visa Europe System, reformat the messages as necessary and deliver them to other systems or networks.

Authorization Gateway Services provide authorization links to the following international card schemes:

- MasterCard
- American Express
- Diners Club International
- Japan Credit Bureau (JCB)
- Discover

In addition, the following are also supported:

- Non-bank cards (for example, cards issued by oil companies)
- Proprietary cards (for example, ATM cards issued by financial institutions, savings and loans, and credit unions)
- Private-label cards (for example, cards issued by department stores)

The Authorization Gateway Service only provides a link to other schemes' authorization processing systems. In a dual message environment, Acquirers will still need to facilitate a connection to the corresponding clearing system. Depending on circumstances, Single Message processing via the Authorization Gateway Service is provided.

Note Scheme rules restrict the clearing of transactions across international borders, so full financial (SMS) messages are not always permitted. Permission may have to be sought from some schemes to allow Visa to process transactions in particular countries. See specific scheme descriptions below for further details.

Visa Europe Authorization Gateway Services provide the following benefits for Members:

- Acquirers use one message format (that is, V.I.P.) for all messages. VEAS converts all non-Visa messages to the appropriate format before routing to the scheme gateway.
- Acquirers can route all requests to Visa Europe rather than to their original destination.
- Acquirers can support multiple card types and payment accommodations using their existing Visa Europe System (Visa card and Plus) connections.
- Redundancy to ensure that alternative switching and routing capabilities are available.
- Support for the Priority Routing Service for SMS Acquirers that access multiple networks. These Acquirers can have VEAS choose the most cost-effective path for their transactions. For information about this service, see [Priority Routing Service](#) on page 245.

- Limited stand-in processing capabilities for American Express and Discover International.
- Stand-in processing for MasterCard issuers that participate in the Visa Shortest Online Path (VSOP) Service (see *Visa Europe Routing Services*).
- Access to SMS processing capability required by regional and national ATM and POS networks.

8.1 International Airline Program

The Visa International Airline Program (IAP) represents an opportunity to enhance service to airlines, improve operational efficiency, and reduce administrative costs by allowing international airline merchants to consolidate their Acquirer relationships in one or a few Acquirer locations.

Authorization Gateway Services enable Visa Europe Acquirers that participate in the International Airline Programme to route non-Visa authorizations through the Visa Europe System.

Note Visa Europe Acquirers wishing to participate in the IAP must submit their business plan for approval along with the Financial Report and Accounts for the airline(s). This data is reviewed by Visa Europe's Fraud and Member Risk departments prior to approval being granted. Any additional markets for an airline already registered must also be approved.

8.2 Related information

For more information about Authorization Gateway Services, see the following documents:

- *Introducing the Visa Europe System*
- *Introducing the Visa Europe Authorization Service*
- *Introducing SMS and DMSA Transactions*
- *Introducing SMS and DMSA Messages*
- *Authorization Gateway Services Cross-Reference Guide*

8.3 Participation

Authorization Gateway Services are available through the dual and single messaging systems to Acquirers in Visa Europe.

Participation is optional and subject to contractual enrolment agreements that specify the Acquirer's responsibilities when accepting cards and processing transactions for non-Visa institutions.

To participate in the services, Members must meet the following requirements.

8.3.1 Testing and certification

To test Authorization Gateway Services, Members must contact their Visa Europe Relationship Manager.

8.3.2 Available gateways

Members can route MasterCard, American Express, Diners Club International, Discover and JCB card authorization requests to the Visa Europe System through their Visa Europe connections. VEAS processes and routes original authorization requests/responses and reversal advices/responses.

American Express and MasterCard transactions are converted by the Visa Europe System into their respective transaction formats before they are forwarded to their networks.

Discover, Diners Club International and JCB transactions remain in Visa's V.I.P. format until they reach their destination networks.

The Visa Europe System delivers the request to the issuer's authorization centre for approval and returns a response to the Member by the reverse path. VEAS does not perform stand in processing for American Express, MasterCard, Diners Club International and JCB transactions. VEAS may provide some limited stand-in processing for Discover transactions.

The following table lists the gateways available to DMSA Members.

Table 4: Gateways available to DMSA Members

Network	Type	Visa Europe availability
Banknet (MasterCard network)	POS and Credit	Available inside and outside the Europe region
American Express Gateway	Credit	Country-dependent
Diners Club International (DCI)	Credit	Country-dependent. Processed by MasterCard's Banknet network.
Japan Credit Bureau (JCB) card	Credit	Country-dependent
Discover	Credit	US
Carte Blanche	Credit	Country-dependent
Proprietary and private-label cards	Credit	Available inside and outside the Europe region

8.3.2.1 MasterCard International

A worldwide contract that supports dual message authorization processing governs the Visa-MasterCard gateway.

Acquirers can send authorization requests for MasterCard POS transactions, including those for electronic commerce and telephone orders, through their Visa Europe System connections to the Visa Europe System, which delivers the requests to Banknet, the MasterCard network, for authorization unless Issuers have established other routing specifications.

Similarly, MasterCard forwards Banknet-acquired Visa authorization requests to the Visa Europe System and delivers responses to Acquirers. For transactions involving multicurrency conversion, Visa Europe Acquirers that participate in the Visa Multicurrency Service can, by default, send and receive their MasterCard transactions in the initially defined local currency.

Other MasterCard services supported:

- Authorizing Agent ID Code
- Payment Initiation Channel
- Promotion Code
- Additional Data, National Use
- MasterCard Assigned ID
- Trace ID
- Transit Program
- Value 34 (Suspect Fraud)

General availability: no special permissions required.

Transactions containing PIN (including ATM): not generally supported.

SMS transactions: supported in some domestic markets (including PIN processing/settlement).

Note Some MasterCard issuers take advantage of Visa Shortest Online Path (VSOP) routing; in such instances authorizations are routed directly to the issuer's processor rather than the gateway.

8.3.2.2 American Express

A worldwide contract exists between Visa and American Express. However, restrictions exist in certain countries; therefore a Member may only use the Visa System for the processing of American Express transactions with prior approval from Visa.

Acquirers can send authorization requests for American Express POS transactions, including those for electronic commerce and telephone orders, through their Visa Europe System connections to the Visa Europe System, which delivers the requests to the American Express Gateway for authorization unless issuers have established other routing specifications.

Similarly, American Express forwards American Express Gateway-acquired Visa authorization requests to the Visa Europe System and delivers responses to Acquirers. For transactions

involving multicurrency conversion, Visa Europe Acquirers that participate in the Visa Multicurrency Service can, by default, send and receive their American Express transactions in the initially defined local currency.

Other American Express services supported:

- American Express instalment payments
- American Express clearing reference data

8.3.2.3 Diners Club International

A worldwide contract, subject to regional/country specific approvals, that supports dual message authorization processing governs the Visa-Diners Club gateway. Visa Europe System-acquired Diners Club authorization requests are routed via the Discover network.

Acquirers can send authorization requests for Diners Club POS transactions through their Visa Europe System connections to the Visa Europe System, which delivers the requests to the Discover network, for authorization unless issuers have established other routing specifications.

Similarly, Diners Club forwards Discover network-acquired Visa authorization requests to the Visa Europe System and delivers responses to Acquirers. For transactions involving multicurrency conversion, Visa Europe Acquirers that participate in the Visa Multicurrency Service can, by default, send and receive their Diners Club transactions in the initially defined local currency.

Other Diners Club services supported:

- Diners Club clearing reference data

8.3.2.4 Japan Credit Bureau (JCB)

A limited contract, subject to regional/country specific approvals, that supports dual message authorization processing governs the Visa-JCB card gateway.

Acquirers can send authorization requests for JCB POS transactions through their Visa Europe System connections to the Visa Europe System, which delivers the requests to the JCB card network, for authorization unless issuers have established other routing specifications.

Similarly, JCB forwards JCB card gateway-acquired Visa authorization requests to the Visa Europe System and delivers responses to Acquirers. For transactions involving multicurrency conversion, Visa Europe Acquirers that participate in the Visa Multicurrency Service can, by default, send and receive their JCB transactions in the initially defined local currency.

8.3.2.5 Discover

A limited contract, restricted to US acquired transactions only, that supports dual message authorization processing governs the Visa-Discover card gateway.

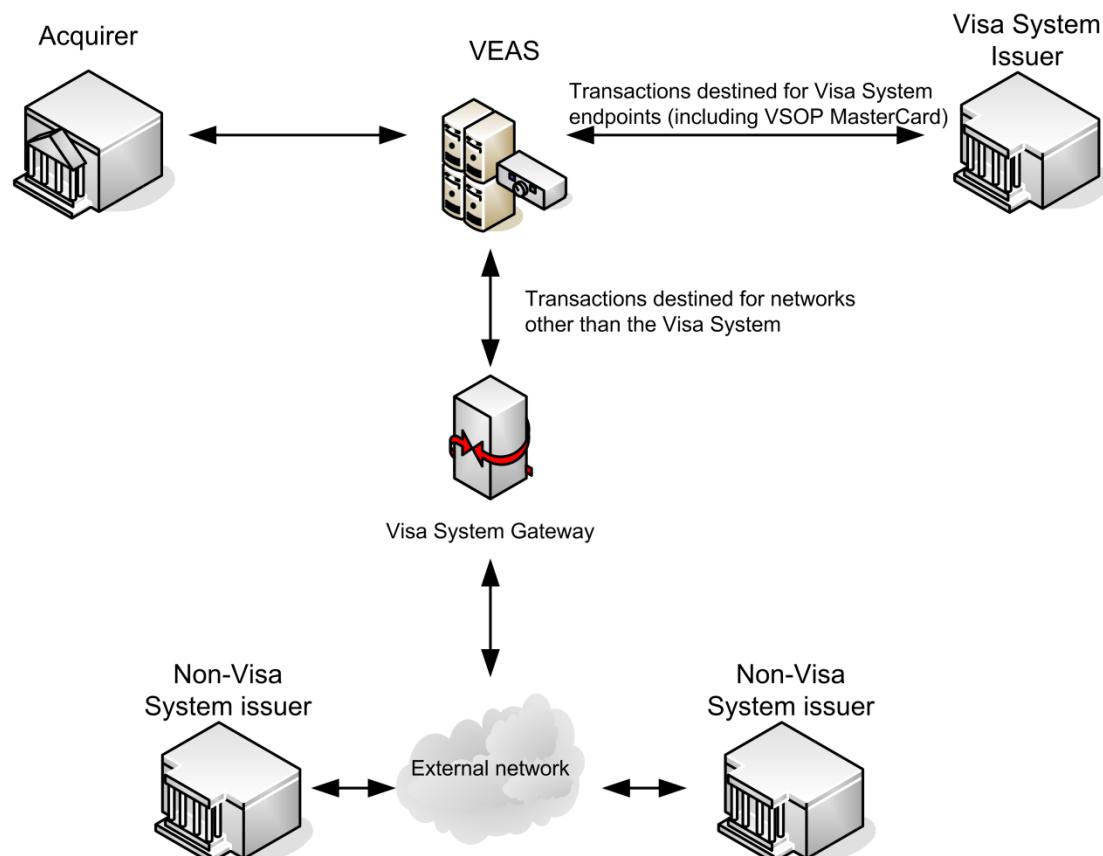
Acquirers can send authorization requests for Discover POS transactions through their Visa Europe System connections to the Visa Europe System, which delivers the requests to the Discover network, for authorization unless Issuers have established other routing specifications.

Similarly, Discover forwards Discover card gateway-acquired Visa authorization requests to the Visa Europe System and delivers responses to Acquirers. For transactions involving multicurrency conversion, Visa Europe acquirers that participate in the Visa Multicurrency Service can, by default, send and receive their Discover transactions in the initially defined local currency.

8.4 Process flows

The following diagram illustrates how the Authorization Gateway Services work.

Figure 15: Process flow for the Authorization Gateway Services



1. The Acquirer sends the request to VEAS.
2. VEAS provides the messages in the appropriate format required by each network:
 - a. American Express, MasterCard: converted to scheme format
 - b. JCB, DCI, Discover, VSOP: V.I.P. format
3. VEAS forwards transactions to the appropriate network gateway based on the account number, the network identification, acquirer reference data and other routing information contained in the message or stored in the Acquirer's system files.

4. Visa Europe receives the authorization response.
5. Visa converts this message to Visa format and forwards to the Acquirer.

8.5 Visa Gateway: Supported transaction types

The following table lists the transaction types that are supported by the Visa Gateway.

Table 5: Visa Gateway: Supported transaction types

Transaction Type	MasterCard	American Express	Diners International	Discover	JCB
Authorization request/response	✓	✓	✓	✓	✓
Authorization reversal/response	Full/Partial	Full	Full/Partial	Full/Partial	Full/Partial
Multicurrency	✓	✓	✓	✓	✓
Stand-in Processing	Decline	Decline	Decline	✓	Decline
PIN-based POS	✓	-	-	-	-
Card Issuer reference data	✓	✓	✓	✓	-
Contactless processing	✓	✓	✓	-	-
Chip data	✓	✓	✓	-	✓
Prepaid/Balance return	✓	✓	-	-	-

9 Balance Inquiry Service

The Balance Inquiry Service enables Cardholders to check their account balance from participating ATMs worldwide.

9.1 Related information

For further information about the Balance Inquiry Service, see the following documents:

- *Single Message System (SMS) ATM Technical Specifications*
- *Single Message System (SMS) ATM Processing Specifications*
- *Dual Message System Authorization (DMSA) Technical Specifications*
- *Dual Message System Authorization (DMSA) Processing Specifications*

9.2 Participation

The Balance Inquiry Service is available through the dual and single messaging systems at participating ATMs.

Participation is:

- Mandatory for Acquirers in Poland
- Optional, but recommended, for all other Issuers and Acquirers

To participate in the service, Members must meet the following requirements.

9.2.1 Issuer implementation considerations

Issuers must meet the following implementation considerations:

- Issuer must be certified.
- Issuer must support balance inquiries as separate, non-financial transactions.
- Issuers establish settings at the Processing Centre level to indicate whether a particular card programme within a Visa System Processor accepts balance inquiries.
- Issuers must provide balances in the currency of the Cardholder's account, for conversion by Visa to the Transaction Currency where appropriate.
- An Issuer must provide the Balance Inquiry Service to Cardholders if it offers balance inquiry services through a network other than its proprietary network.
- If an Issuer does not participate in the service, any inquiry from its Cardholders will be declined and a decline fee will be assessed. See the applicable payment scheme or processing rules.

9.2.2 Acquirer implementation considerations

Acquirers must meet the following implementation considerations:

- Acquirer must be certified
- Acquirer must support balance inquiries as separate, non-financial transactions
- Acquirer must display balance information at minimum in the Acquirer currency, and optionally in Issuer currency if different and where appropriate
- Acquirer may additionally provide Cardholders with any balance information provided by the Issuer as part of an ATM cash disbursement
- Because there is no settlement between Acquirers and Issuers, inquiry transactions cannot be reversed, adjusted, charged-back, or represented
- A participating (ATM) Acquirer receives a fee for each balance inquiry as specified in the applicable payment scheme or processing rules
A fee will be assessed for each balance inquiry request irrespective of the associated Issuer's participation in the service
- An Acquirer must provide the Balance Inquiry Service to Cardholders if it offers balance inquiry services through a network other than its proprietary network

9.2.3 Testing and certification

Certification is mandatory for Issuers and Acquirers.

Visa Member Testing Service (VMTS) provides testing and certification assistance for Members. For more information, Members should contact Visa Europe Customer Support.

9.2.4 Service monitoring

There is no monitoring for the Balance Inquiry Service.

9.2.5 Planning and implementation

Participation in the service, for both Acquirers and Issuers, is a Member parameter option maintained by Visa Europe. To participate, Members must complete a *Member Information Questionnaire* detailing the requirement and successfully complete all certification requirements.

For more information, Members should contact Visa Europe Customer Support.

9.3 How the service works

In addition to being able to request an account balance from a domestic ATM, it is also possible to request a balance at a non-domestic ATM; irrespective of whether that ATM uses the same or a different currency. The procedure for requesting such a balance remains the same, however, where applicable, additional data is provided by Visa to manage currency conversion.

It is a prerequisite that both the Acquirer and the Issuer participate in the service.

The following process illustrates how a balance request is progressed:

1. Cardholder requests an account balance at an ATM.
Balances can be requested for all cards.
2. Acquirer creates a balance request and sends it to VEAS.
The message is flagged to indicate that it is an inquiry.

Data field 3, processing code			
Field/ Position	Name	Value	Description
3/ 1-2	Processing Code Transaction type	30	Balance, available funds inquiry

3. VEAS forwards the balance request to the Issuer.

If the Issuer is not available, after checking the Exception File, stand-in processing (STIP) responds directly to the Acquirer with an 'Issuer unavailable' response. STIP cannot process balance inquiries because it does not have access to the relevant account data.

4. Issuer determines the balance details and sends a balance response to VEAS.

Data field 54, additional amounts			
Field	Name	Value	Description
54	Additional Amounts	n(12)	Account balance

5. VEAS edits the balance response, and where appropriate, converts the balance information from the Issuer's currency to the Acquirer's currency, populates the additional information in the message, and then forwards the response to the Acquirer.
6. Acquirer routes the balance response to the ATM.
7. ATM displays the balance(s).

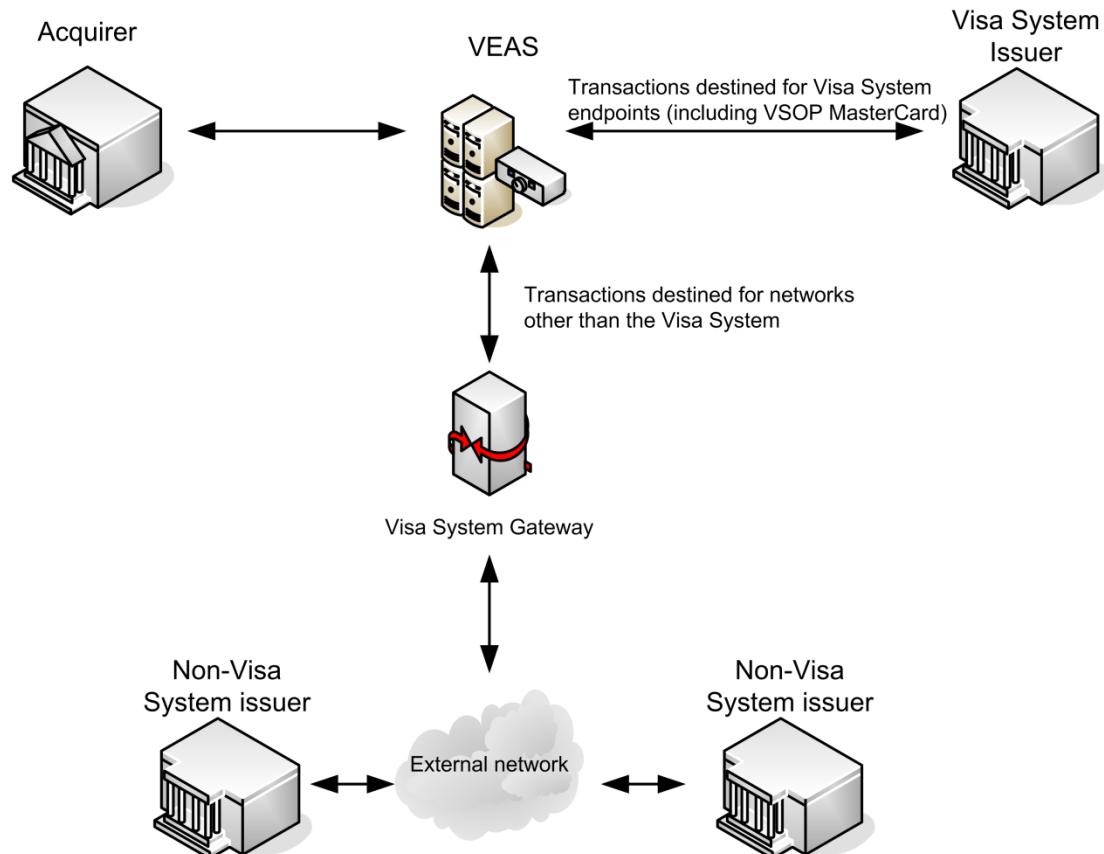
9.3.1 Stand-in processing

Stand-in processing is not used. All inquiries are forwarded to the Issuer.

9.4 Message flow

The following diagram illustrates the message flow for the Balance Inquiry Service.

Figure 16: Message flow for the Balance Inquiry Service



1. Balance request raised by Acquirer.
2. Balance response returned by Issuer.

9.5 Key messages

The following messages carry the Balance Inquiry Service:

- 0100, 0200 balance inquiry request
- 0110, 0210 balance inquiry response

9.6 Key data fields

The following key data fields are used by the Balance Inquiry Service. For detailed information, see the Visa Europe technical specifications.

Data field 3 - Processing Code

This field identifies the transaction type. The account type may also be specified.

Inclusion of '30' as transaction type is mandatory. If an account type is specified, the value must match the account type detailed in field 54.

Data field 54 - Additional Amounts

This field contains account balance details. The data returned to the Acquirer depends on whether multicurrency is involved, for example, where a Cardholder requests a balance at a non-domestic ATM. For multicurrency inquiries, amounts are displayed in the currency of the ATM.

10 Bilateral Interchange Fee Processing Service

The Bilateral Interchange Fee Processing Service operates where a participating Acquirer and Issuer agree to exchange bespoke Interchange Reimbursement Fees under a private agreement. The fees are settled and reported as normal by the Visa Europe Settlement Service (VSS). This service enables Members to meet specific business needs such as domestic Interchange Reimbursement Fee legal requirements.

Bilateral Interchange Reimbursement Fees are bespoke fees that are agreed between an Acquirer and Issuer, which:

- Supersede multilateral Interchange Reimbursement Fees
- Are settled and reported as normal in VSS

Important These fees must be kept strictly confidential between the two participating Members.

For transactions where a bilateral Interchange agreement does not apply, the multilateral Interchange Reimbursement Fees published by Visa Europe must be used.

Bilateral Interchange reimbursement works in the same way as other Interchange Reimbursement Fee calculations (for more information, see *Interchange Reimbursement Fee Processing Service* on page 165), but only applies to specific Members of a particular agreement.

10.1 Related information

For further information about the Bilateral Interchange Fee Processing Service, see the following documents:

- *Visa Europe Fee Guide*
- *Visa Europe Merchant Data Standards Manual*
- For Visa Europe interchange fee levels, see the Visa Europe web site:
www.visaeurope.com

For details, contact Visa Europe Processing Services.

10.2 Participation

The Bilateral Interchange Fee Processing Service is available through the Visa Europe Clearing and Settlement Service (VECSS).

Participation is optional for Members and their Processors.

Important Due to the confidential nature of bilateral agreements, if you want to participate in the Bilateral Interchange Fee Processing Service, contact Visa Europe Processing Services for more information.

When planning to set up a bilateral agreement, consider the following points should be considered:

- Bilateral agreements can apply to all transactions or to only certain transactions
- Fees can be set up at BIN, product, programme, ATM/POS and Merchant Category Code (MCC) level and can be bi-directional if Members are both Acquirer and Issuer
- Bilateral agreements can involve domestic transactions, Visa Europe transactions or International transactions
- Fees are reported in settlement Interchange (VSS 130) reports
- Bilateral Interchange fees can be a percentage, a flat rate or a combination of both

If you want to amend an existing bilateral agreement, for example by adding a BIN or deleting it from the agreement, contact Visa Europe Processing Services.

11 Card Recovery Bulletin Service

The Card Recovery Bulletin Service enables an Issuer to notify Acquirers of blocked account numbers. It helps protect Issuers from below-floor limit transactions, which do not require authorization, and are not subject to an account check. The service generates an electronic listing (bulletin) of blocked account numbers using data contained in the Exception File, with the relevant listing code, for Dual Message System Authorization (DMSA).

Bulletins are generated on a weekly basis, as per the schedule published in the *Card Recovery Bulletin (CRB) User's Guide*. The bulletin warns Acquirers and Merchants of cards that Issuers no longer honour and want picked up.

Issuers indicate which accounts are to be listed in a bulletin (and for how long) by flagging the requisite accounts in the Exception File (see [Exception File](#) on page 88). Separate bulletins are created for each Visa region (excluding the USA, where the service is not supported). It is possible to list an account on more than one regional bulletin if required (for more information, see [CRB service regions](#) on page 89).

Issuers receive chargeback protection for listed account numbers for the duration of the effective period of the bulletin. For any transaction which is below the floor limit and takes place using a card that is listed on the bulletin, and has a Transaction Date during the effective period of that bulletin, the Issuer will have the right to dispute the transaction via a chargeback.

Participating Acquirers receive an electronic copy of bulletin listings via the Regional Card Recovery File (RCRF), which is delivered weekly as part of the Visa Europe Clearing and Settlement Service (VECSS) incoming Interchange File.

In addition to bulletin listings, the RCRF also includes details of Exception File records that have been added, purged (see [Purge date](#) on page 89) or amended since production of the current effective bulletin. It also includes details of any blocked BINs, and counterfeit, lost and stolen card numbers. However, liability protection offered to Issuers is based only on effective bulletin listings.

Acquirers are responsible for passing on the information in the RCRFs to their Merchants.

In summary, the Card Recovery Bulletin Service:

- Uses the information in the DMSA Exception File to identify account numbers of accounts that Issuers do not want to honour or that require card pick-up
- Produces and distributes weekly electronic files
- Produces billing reports and calculates distribution charges
- Supports account verification for transactions below floor limits

11.1 Related information

For additional information about the Card Recovery Bulletin Service, see the following documents:

- *Card Recovery Bulletin Service (CRB) User's Guide*
- *Visa Europe System Management for Members*

11.2 Participation

The Card Recovery Bulletin Service is available through VECSS to users of dual message processing and SMS that process unauthorized, below-floor limit transactions.

Note The service is not relevant to online transactions.

Participation is optional for Members. It is available to Merchants whose Acquirers participate in the service.

To participate in the service, Members must meet the following requirements.

11.2.1 Testing and certification

Certification is not required for participation in the Card Recovery Bulletin Service.

To test this service, contact Visa Europe Customer Support.

11.2.2 Service monitoring

There is no monitoring for the Card Recovery Bulletin Service.

11.2.3 Planning and implementation

To receive a weekly Regional Card Recovery File, an Acquirer must complete an *RCRF Request Form*. A copy of this form is available in the *Card Recovery Bulletin (CRB) User's Guide*. For further details, contact Visa Europe Customer Support.

11.3 How the service works

11.3.1 Card recovery bulletin (CRB)

Bulletins are effective for one week. The cut-off point for receipt of bulletin items is the Monday evening prior to the effective date. The bulletins are distributed the following day as part of a Regional Card Recovery File, and become effective on the Saturday of the same week (for certain countries in the Asia Pacific region, the effective date is Sunday). Each issue is valid until the effective date of the next issue. Each new issue invalidates all previous issues. (See *Exception File* on page 88.)

The CRB production schedule is pre-determined and published in the *Card Recovery Bulletin (CRB) User's Guide*. Issues are numbered in sequence from 01-01A to 99-99A; on the hundredth publication in a sequence, the issue number returns to 01-01A.

Acquirers are responsible for passing on the content of a CRB to their Merchants.

Figure 17: Chart showing the production date and effective periods for bulletins 92-94

23/01/2012 - 24/02/2012						
Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
January 23	24	25	26	27	28	29
 20:00 GMT Issue 92 in preparation and distributed on Tuesday via RCRF					Issue 92 Effective	
30	31	February 1	2	3	4	5
 20:00 GMT Issue 92A in preparation and distributed on Tuesday via RCRF					Issue 92A Effective	
6	7	8	9	10	11	12
 20:00 GMT Issue 93 in preparation and distributed on Tuesday via RCRF					Issue 93 Effective	
13	14	15	16	17	18	19
 20:00 GMT Issue 93A in preparation and distributed on Tuesday via RCRF					Issue 93A Effective	
20	21	22	23	24	25	26
 20:00 GMT Issue 94 in preparation and distributed on Tuesday via RCRF					Issue 94 Effective	

The service extracts data from the DMSA Exception File. A bulletin includes account numbers with an action pick-up code **and** a CRB region code of A-F, indicating inclusion in a particular regional bulletin or bulletins.

The bulletins in which an account number will be listed depend on its associated pick-up code, CRB service region code and the purge date of the Exception File record.

Table 6: Account number listing dependencies

Exception File				Bulletin (issue / region code)					
Account number	Pick-up code	Region code	Purge date	92	92A	93	93A	94	94A
account1	41	0	30-Jan-12	N	N	N	N	N	N
account2	41	E	24-Jan-12	Y	N	N	N	N	N
account3	43	E	14-Mar-12	Y	Y	Y	Y	Y	Y
account4	43	E,F	17-Feb-12	Y	Y	Y	Y	N	N
account5	04	F	02-Feb-12	Y	Y	N	N	N	N
account6	04	F	12-Apr-12	Y	Y	Y	Y	Y	Y
Region E = Europe Region F = Latin America and Caribbean 0 = no regional listing Y = indicates that account will be listed, N that it will not									

11.3.2 Regional Card Recovery File

Bulletins are distributed directly to subscribers (Acquirers) on a weekly basis via the Regional Card Recovery File (TC 55 - RCRF update transaction records), as part of their VECSS incoming Interchange. An RCRF includes:

- CRB listings (account numbers included in a particular regional CRB)
- Account numbers listed as counterfeit, lost, or stolen
- Blocked BINs
- Range of blocked BINs
- Updated Exception File records: this may include items not on a current CRB, but waiting for listing on the next effective CRB

All data is updated weekly.

11.3.3 Fees and billing reports

Issuers pay a fee for listing an account number on a regional bulletin. The fee is per account number, per issue, per regional bulletin. A fee is also payable for blocking a BIN or BINs. Members pay a fee to receive an RCRF. The Card Recovery Bulletin Service produces billing reports and calculates distribution charges on a monthly basis.

For more information on fees, see the *Visa Europe Fee Guide*.

11.3.4 Exception File

The Exception File is a file of account numbers for which the Issuer has pre-determined the authorization response. The Visa Europe Authorization Service (VEAS) maintains separate Exception Files for DMSA and SMS. However, the Exception File for DMSA is the only source of input to the CRB. If Issuers that use SMS want to list accounts in the CRB, the relevant records must also exist in the Exception File for DMSA. Consequently, SMS accounts may be included in the Exception Files for both DMSA and SMS. Issuers are responsible for the content and maintenance of the Exception File, and must keep it up-to-date.

For more information about maintaining the Exception File, see the *Visa Europe System Management for Members* manual.

Issuers flag an account for inclusion in a bulletin by updating the Exception File, and ensuring the following key data is included:

- The account number
- An action code indicating 'pick-up'
- The date that the Visa Europe System should purge the Exception File record
- The applicable CRB service region(s)

11.3.4.1 Account number

Only account numbers of between 9 and 19 characters in length are included in a bulletin. account numbers outside this range may be included in the Exception File, but will not be included in the bulletin.

11.3.4.2 Action code

Action codes indicating card pick-up are listed in the following table.

Table 7: Exception File action codes

Action code	Action	Description	Type
04	Pick-up card	Unspecified	Non-fraud
07	Pick-up card	Special conditions (other than lost, stolen or counterfeit card)	Fraud
41	Pick-up card	Lost card	Fraud
43	Pick-up card	Stolen card	Fraud

11.3.4.3 Purge date

The purge date determines how long a listed account should remain on the Exception File. The date takes account of bulletin effective dates to ensure that an account remains on file for any period that it is included in a bulletin. For example, if a purge date falls during a bulletin effective period, the purge will not take place until the next bulletin becomes effective.

11.3.4.4 CRB service regions

A CRB region code identifies a specific regional bulletin. Issuers usually assign a single code to each affected account number. However, accounts can be allocated multiple region codes if required; and a card's inclusion in a bulletin is not dependent on the geographical location of its Issuer. The CRB region codes are listed in the following table:

Table 8: CRB service regions

CRB region code	Region
0	Do not list in any card recovery bulletin. The account will only be listed in the Exception File
A	Asia-Pacific
B	Central and Eastern Europe, Middle East and Africa
C	Canada
D	National card recovery bulletin (NCRB). Before Visa can produce an NCRB, all Acquirers within the country must agree to its use. Agreement among Acquirers is necessary to avoid chargeback disputes arising when both regional and national CRBs are used in the same country. For further information, see the <i>Card Recovery Bulletin (CRB) User's Guide</i> .

Table 8: CRB service regions (continued)

CRB region code	Region
E	Europe
F	Latin America and Caribbean
Y	All CRB regions (A, B, C, E, F)
Z	All CRB regions (A, B, C, E, F)

11.3.4.5 Exception File update deadline

The cut-off time for including Exception File updates for account numbers to be listed in a bulletin, is 20:00 GMT on the Monday preceding the bulletin effective date. Updates that miss this deadline are included in the next bulletin. Issuers request updates by submitting 0302 Issuer File Update Requests.

11.3.4.6 Exception File reports

A number of reports are available, including BIOSR112 Exception File Listing, which detail Exception File content. For more information, see the *SMS and DMSA System Reports* document.

11.3.5 Chargeback Reduction Service

The Chargeback Reduction Service (CRS) operates for clearing transactions, and validates original purchase and cash transactions, as well as certain chargebacks, against the appropriate Card Recovery Bulletin. CRS only considers transactions that are below the floor limit for a Merchant. CRS checks whether an account number was listed on a bulletin effective on the Transaction Date.

For more information on this service, see [Chargeback Reduction Service](#) on page 110.

11.3.6 Best practice

The following are offered as best practice guidelines to Issuers using the CRB:

- List account numbers that are either lost or stolen outside the issuing region or country, or which have confirmed fraudulent activity from a foreign region or country, in the appropriate CRB for an initial listing.
- Either every one or two weeks, on Friday or Monday, review all accounts listed on the CRB for continued activity. Ensure that this is done just before the Monday cut-off period for bulletin listings. Extend listings for those cards that remain active with attempted or posted transaction activity from foreign regions.
- Monitor activity that includes decline responses; items returned by the Chargeback Reduction Service (CRS), and posted transactions.
- Review the monthly CRS report, *CBRMR301 - An Issuer Perspective*, to determine transactions returned by CRS.

- Remove cards from the bulletin if no activity occurred over the past two weeks or if all cards have been confiscated.
- For temporary fraud situations, BIN range blocking is possible in the CRB. Evaluate the costs associated in publishing cards in the CRB against the benefits received.
- For cards that are excessively active at specific Merchants, identify the Acquirer through the Visa Interchange Directory and contact the Acquirer's security department to request assistance in having the card confiscated.

The following are offered as best practice guidelines to Acquirers:

- Implement a process to download and distribute RCRFs to Merchants on a weekly basis
- Educate Merchants on how to use an RCRF
- Validate that Merchants are using the RCRFs

11.4 Process flow

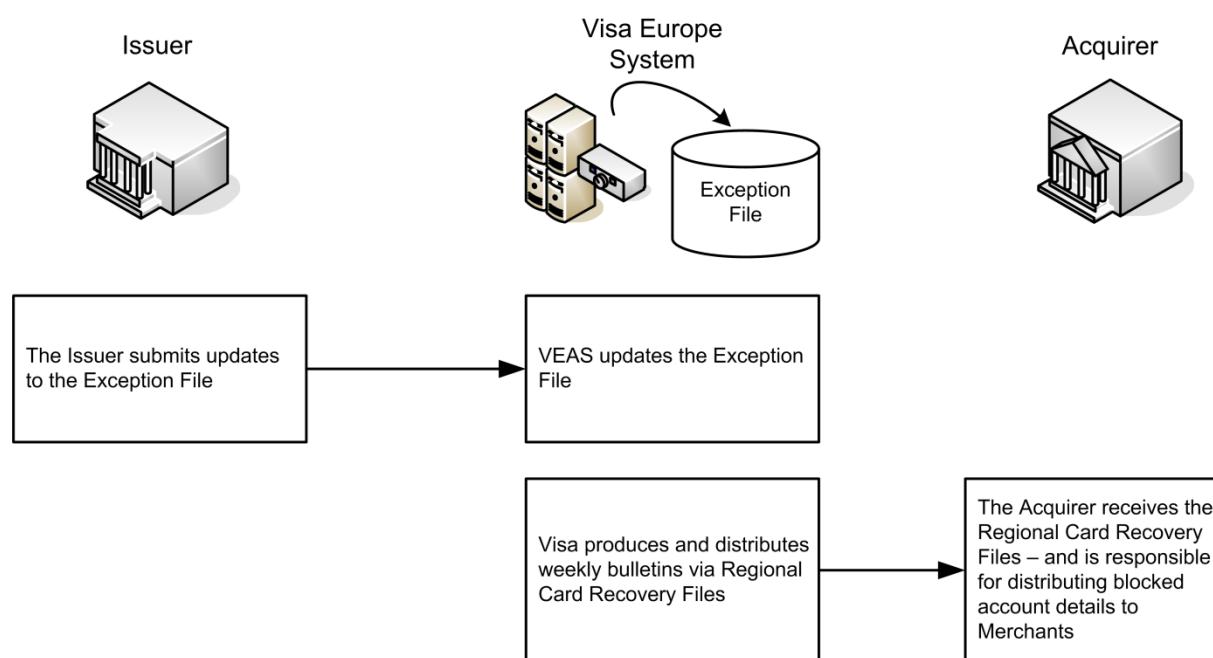
This section describes the process flows for the Card Recovery Bulletin Service.

11.4.1 CRB process flow

To list an account in a bulletin, Issuers request an Exception File update. The Card Recovery Bulletin Service combines the bulletin listings with account numbers of counterfeit, lost, or stolen cards and blocked BINs, to produce Regional Card Recovery Files. Visa distributes the Regional Card Recovery Files as part of the weekly Interchange File.

The following diagram illustrates the Card Recovery Bulletin Service process flow.

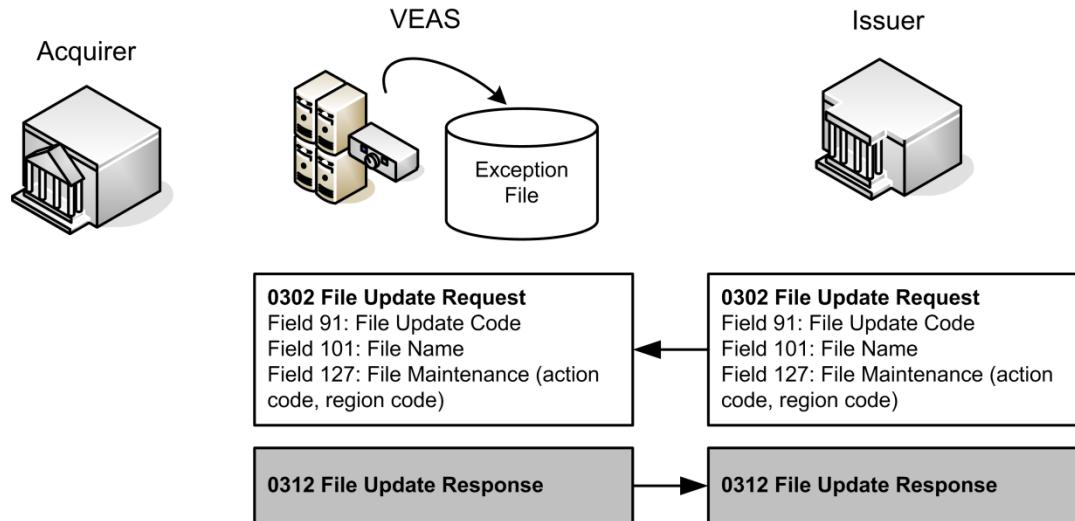
Figure 18: CRB process flow



11.5 Key messages

The following messages are relevant to the Card Recovery Bulletin Service. 0302 requests are the only messages that can be used to allocate a CRB region code.

Figure 19: Key messages for the Card Recovery Bulletin Service



- **0302 Issuer File Update Request**

This message is a request to update (add, change, delete) or to retrieve the information in a cardholder record stored in the Exception File. VEAS generates a 0312 response.

- **0312 Issuer File Update Response**

This message is the response to a 0302 File Update Request. A File Update Response indicates whether VEAS performed the requested maintenance.

- **TC 55 - RCRF Update Record Transactions**

VECSS uses this transaction code to transmit updates to the Regional Card Recovery File (RCRF).

11.6 Key data fields

The following key data fields are relevant to the Card Recovery Bulletin Service. For detailed information, see the Visa Europe technical specifications.

Data field 73 - Date, Action

This data field indicates the record's purge date, for Add/Change File Update Requests. It is not required in Delete Requests.

Data field 91 - File Update Code

This data field indicates the type of file processing required in 0302 update messages affecting Cardholder Database files. Field 91 is required in all 0302 requests.

Data field 101 - File Name

This data field identifies which Exception File is to be updated in a maintenance request. VEAS maintains separate Exception Files for DMSA and SMS. However, the Exception File for DMSA is the only source of Exception File input to the CRB. If Issuers that use SMS want to list accounts on a CRB, the records must also exist in the Exception File for DMSA. Consequently, SMS accounts may be listed in the Exception Files for both DMSA and SMS.

Data field 127 - File Maintenance

This data field is used in 0302 Exception File Update Requests. It is required in file Add and Change requests, but is not required in Delete requests. When present in a File Update Request, it is also returned in the complementary 0312 response.

12 Card Verification Service

The Card Verification Service is a service that validates cards when used in purchase and cash transactions. The Card Verification Service provides protection to Issuers and Acquirers:

- From fraud losses that are associated with counterfeit Visa cards
- Against skimming of the magnetic stripe data to a counterfeit card
- To reduce fraud losses on card-absent transactions

12.1 Implementations

This service has a number of implementations:

- Card Verification Value (CVV) on magnetic stripe cards
 - Provides protection for an Issuer and an Acquirer against magnetic stripe counterfeit. It enables an Issuer to verify the unique CVV encoded on the magnetic stripe to detect invalid cards.
 - integrated Chip Card Verification Value (iCVV) on chip cards
 - Provides protection for an Issuer and an Acquirer against skimming of the Magnetic Stripe Image (MSI) data from the chip to a counterfeit magnetic stripe card. The iCVV protects chip-based transactions.
 - Card Verification Value 2 (CVV2) on card-absent transactions
 - Helps protect the Issuer from counterfeit fraud in card-absent environments (since the CVV2 is physically printed on the back of the card and not available elsewhere). Hence it reduces fraud losses and the risk of the Cardholder not having the physical card. The CVV2 protects card-absent transactions.
 - dynamic Card Verification Value (dCVV) on contactless chip cards
 - Provides protection at point-of-sale (POS) and ATM to Issuers and Acquirers from fraud losses associated with counterfeit Visa cards. The dCVV protects contactless chip-based transactions.
- Note** Currently, contactless transactions are processed offline. However Members are expected to meet dCVV standards.

12.1.1 Basic processing principles

The basic processing principles are the same across all implementations. In every service, a three-digit verification value is calculated from the key inputs. There is one standard algorithm used to calculate the CVV, iCVV, dCVV and CVV2 values, however the inputs for CVV, iCVV, dCVV and CVV2 are slightly different. The key inputs are:

- Account number (PAN)
- Service code
- Expiry date
- Card Verification Key (CVK) or Master Derivation Key (MDK)

The first three inputs are part of the authorization data in a transaction. The CVK (or MDK) is held by VEAS (where the Issuer has elected for Visa Europe to verify CVVs) to validate the CVV. Variations in the usage of the inputs ensure that each of the three-digit codes generated for the Card Verification Service is different.

12.2 Related information

For additional information about the Card Verification Service, see the following documents:

- *Payment Technology Standards Manual*
- *Visa Smart Debit/Credit (VSDC) Acquirer Implementation Guide*
- *Visa Smart Debit/Credit (VSDC) Issuer Implementation Guide*
- *Visa Contactless Issuer Member Implementation Guide*
- *VisaNet Certification Management Service, Testing and Certification Guide - Visa Authorization System*
- *Introducing the Visa Europe Authorization Service*
- *Dual Message System Authorization (DMSA) Technical Specifications*
- *Single Message System (SMS) ATM Technical Specifications*
- *Single Message System (SMS) POS Technical Specifications*
- *Visa Smart Debit/Visa Smart Credit System Technical Manual*
- *PCI Data Security Standards*
- *Dual Message System Authorization (DMSA) Processing Specifications*

12.3 Participation

The Card Verification Service is available to all Members and their Processors with magnetic stripe, contact and contactless chip and card-absent transactions using CVV, iCVV, dCVV and CVV2. The following participation requirements apply:

- CVV and iCVV are mandatory for Issuers
- dCVV is optional for Members, Issuers, Acquirers and their Processors with contactless cards

Note The Card Verification Service is used by all Acquirers.

12.3.1 Participation requirements for Issuers:

To participate in the service, an Issuer must:

- Provide CVKs and MDKs for dCVV, the expiry dates to which each of these keys relates, card verification processing options (such as ALL, ALL RESPOND, STIP ONLY) and the default response codes for verification failure
- Demonstrate that CVV, iCVV, CVV2 and dCVV are correctly calculated
- Demonstrate that CVV, iCVV and dCVV are placed correctly on the magnetic stripe and in the chip

- Ensure that the cards have valid expiry dates

Important The Visa Security Module (VSM) allows the Issuer to use the 'MMYY' or 'YYMM' date format to calculate the CVV2. During the enrolment and certification process, a participating Issuer must indicate which date format they use so VEAS can correctly calculate the CVV2 for each Issuer. For CVV, iCVV and dCVV they must use 'YYMM' date format.

- Use Data Encryption Standard (DES) keys

The following table describes each of the processing options and which service can use them.

Table 9: Processing options for CVV, iCVV, dCVV and CVV2

Service	Processing option
CVV, iCVV and dCVV	<p>ALL - VEAS verifies the CVV/iCVV/dCVV on all eligible transactions and forwards the results to the Issuer in the request messages.</p> <p>ALL RESPOND - VEAS verifies the CVV/iCVV/dCVV, on all eligible transactions. If the verification fails, VEAS responds to the Acquirer with the Issuer's invalid CVV/iCVV/dCVV response code (or a more severe response code determined by stand-in processing (STIP), if applicable). VEAS also creates an advice message informing the Issuer of the CVV/iCVV/dCVV results.</p> <p>STIP ONLY - VEAS verifies the CVV/iCVV/dCVV when STIP processes the transaction. If verification fails and if no other, more severe response code is assigned to the transaction, STIP responds to the Acquirer with the Issuer-provided CVV/iCVV/dCVV invalid response code and indicates that the CVV/iCVV/dCVV verification failed in the advice message to the Issuer.</p> <p>Note This option is the minimum requirement which ensures that the CVV/iCVV/dCVV can be checked always, irrespective of Issuer availability.</p> <p>NONE (Issuer-only validates) - The Issuer verifies all CVV/iCVV/dCVVs. If the Issuer is unavailable, STIP does not check the CVV/iCVV/dCVV. This option means that VEAS always routes the authorization request directly to the Issuer without checking the CVV/iCVV/dCVV.</p>
CVV2	<p>ALL - VEAS verifies the CVV2 for all eligible transactions and forwards the response to the Issuer in the authorization request.</p> <p>NONE (Issuer-only validates) - VEAS does not verify the CVV2; it forwards authorization requests to the Issuer for CVV2 verification.</p>

In addition, participating Issuers must also comply with the following requirements for using dCVV:

- A dCVV must be embedded in the magnetic stripe data in the last four bytes of the Issuer Discretionary Data (IDD).
- Issuers must modify their systems to:
 - Support the full set of transactions initiated for contactless.
 - Provide the capability to process the unique value of the IDD that was provided by the contactless chip card in the authorization request. The IDD in the contactless

card is used to ensure accurate processing of the dCVV when the transaction is initiated.

- Issuers must provide Visa Europe with a STIP default response code. '00' (approval) is not allowed.
- The contactless chip cards must have the capability to support qVSDC, dCVV contactless payment processing, contact chip and the normal POS processing of magnetic stripe transactions.

For more information see the *Visa Contactless Issuer Member Implementation Guide*.

12.3.2 Participation requirements for Acquirers

The Card Verification Service is available to all Acquirers and their Processors.

To participate in the service, the Acquirer must demonstrate the ability to:

- Transmit the complete magnetic stripe or chip data in Track 1 (or Track 2) indicating this with a valid code in data field 22.1, from any physical terminal (CVV, iCVV only).
- Transmit the CVV2 presence indicator, CVV2 return flag and the CVV2 value in the authorization request (CVV2 only).
- Receive data field 44.5 - CVV/iCVV Results Code, if they select that option (CVV/iCVV/dCVV only).
- Ensure a dCVV is embedded in the magnetic stripe data in the last four bytes of the Issuer Discretionary Data (IDD) (dCVV only).
- Modify their systems to provide the capability to process the unique value of the IDD that was provided by the contactless chip card in the authorization request. The IDD in the contactless card is used to ensure accurate processing of the dCVV when the transaction is initiated. (dCVV only).

12.4 General Processing requirements

To participate in Card Verification Service processing, Members must meet the following conditions:

- The POS or ATM environments must support:
 - The capture of the magnetic stripe
 - The capture of qVSDC chip data, including the MSI
 - Electronic authorization by VEAS or the Issuer
 - Contactless transactions (qVSDC only)
 - Processing capabilities for DMSA or SMS message types
- An Acquirer must provide complete magnetic stripe or chip data (either from the Magnetic Stripe or the MSI in the chip) in 0100 authorization messages and 0200 financial messages

- Issuers must place the CVV or iCVV correctly on Track 2 (and Track 1) of the magnetic stripe, chip or contactless card
- The CVV2 must be clearly visible on the card signature panel
- For dCVV, the IDD field in the track data of contactless cards contains both the computed dCVV and the current Application Transaction Counter (ATC)
- The content of the magnetic stripe and the MSI in the chip must be identical, (except when the chip MSI contains an iCVV)

Important If an iCVV from the chip MSI has been used to create a fraudulent magnetic stripe, any subsequent CVV verification fails because the magnetic stripe and the chip MSI have different values.

12.4.1 Additional processing requirements for dCVV

In addition to the conditions for CVV, iCVV, CVV2 and dCVV, dCVV processing is successful under the following conditions:

- Participants in dCVV must first also participate successfully in CVV
 - Contactless cards wanting to perform dCVV must adhere to Visa specifications, in particular the use of Visa-defined IDD on Track 2
- Note** The IDD incorporates the ATC for contactless transactions.

12.5 Requirements for checking card verification values

This section describes the requirements for checking card verification values.

12.5.1 CVV, iCVV and dCVV

Checking the CVV, iCVV and dCVV requires the following:

- Both the Acquirer and Issuer are Card Verification Service participants
- The POS Entry Mode contains the correct value
- The full magnetic stripe or chip data must be included in the appropriate data field for Track 1 and/or Track 2
- The expiry dates printed on the cards or encoded on the magnetic stripe

12.5.2 CVV2

Checking the CVV2 requires the following:

- The PAN and expiry date only
- The POS Entry Mode indicates a card-absent transaction
- Data field 126.1 must contain the CVV2

12.6 Testing, monitoring and implementation requirements

12.6.1 Testing and certification

To participate, Visa Europe requires certification for the Card Verification Service. The Visa Member Testing Service (VMTS) for VEAS provides testing and certification assistance for Card Verification Service participants.

Certification demonstrates the ability to support the Card Verification Service requirements.

To arrange testing and certification for the Card Verification Service, contact Visa Europe Customer Support.

12.6.2 Service monitoring

Service monitoring is not available for the Card Verification Service.

12.6.3 Planning and implementation for an Issuer

An Issuer that participates in the Card Verification Service using CVV, iCVV, CVV2 and dCVV must modify how they process authorization requests, authorization response and advice messages to support the service.

To prepare for Card Verification Service participation, the Issuer must first:

- Choose the track location for the CVV, iCVV, dCVV and inform Visa Europe of the location
- Calculate and encrypt CVV, iCVV, dCVV and CVV2
- Establish the service start date
- Provide Visa Europe with CVK and/or MDK encryption keys
- Provide expiry date format for CVV2, that is, YY/MM or MM/YY

For full planning and implementation support, contact Visa Europe Customer Support.

12.6.4 Planning and implementation for an Acquirer

An Acquirer that participates in the Card Verification Service using CVV, iCVV and CVV2 must modify authorization request and authorization response formats to support the service.

To prepare for Card Verification Service participation, the Acquirer must first:

- Prepare a CVV, iCVV and CVV2 enrolment form for contact information
- Complete a Member Information Questionnaire for scheduling implementation activities
- Check whether new terminal software or downloads are required to support the capture and transmission of the complete magnetic stripe or chip data and its associated indicator

For full planning and implementation support, contact Visa Europe Customer Support.

12.6.5 Ongoing maintenance and enhancement of the Card Verification Service

From time to time, there is a need to add, change or delete CVV, iCVV, dCVV or CVV2 related BIN parameters and keys used by the Card Verification Service. For ongoing maintenance and enhancement, contact Visa Europe Customer Support.

12.7 How the service works

All the verification services described in this manual use the same underlying methodology. A verification value is determined by providing three basic elements and cryptographically manipulating these elements with a CVK to produce a unique verification value. Detailed information can be found in the *PCI Data Security Standards* document, but the main procedures are described here.

The three basic data elements used for card verification are:

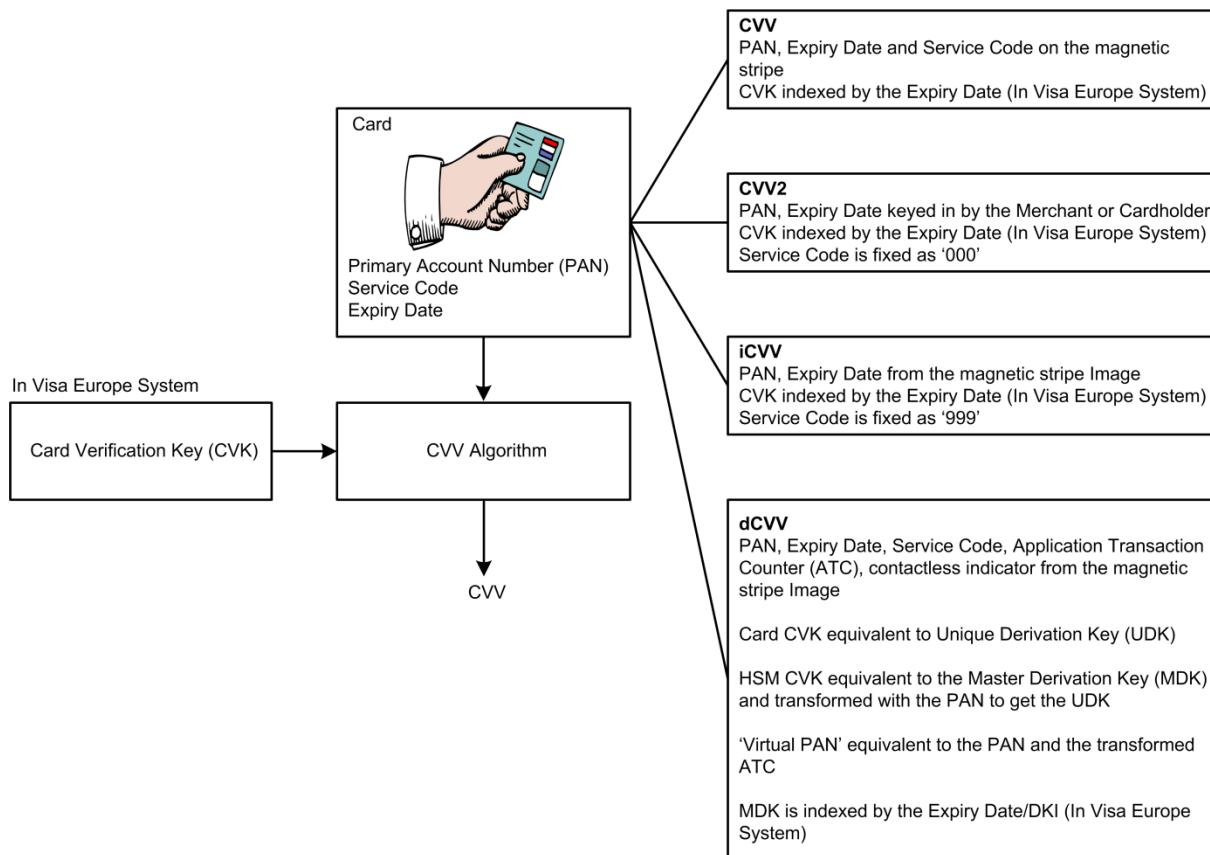
- Primary account number (PAN)
- Service code
- Expiry date

The CVK is a double-length DES key value. Issuers provide the CVK or MDK to Visa Europe so that VEAS is able to perform card verification as determined by the Issuer.

The output from the cryptographic manipulation of the basic data elements with the CVK, is the three-digit CVV.

During the transaction authorization process, VEAS or the Issuer regenerates a unique verification value using the basic data elements and compares it to the verification value provided in the authorization request. If the two are equal, the system gives a positive response.

The following diagram illustrates where each of the key elements are held and which element is used to calculate each verification value.

Figure 20: How the Card Verification Service works

The basic elements and comparison verification value are derived as follows:

- CVV - from the magnetic stripe
- iCVV/dCVV - from the MSI or chip
- CVV2 - keyed by Merchant or Cardholder

12.7.1 Service code

In order to ensure that the verification values differ from each other, the service code is varied as follows:

- CVV/dCVV - from the magnetic stripe (image)
- iCVV - default value of '999'
- CVV2 - default value of '000'

12.7.2 Expiry date

The expiry date is provided to the verification algorithm in 'YYMM' format from the magnetic stripe, or image of the magnetic stripe in the case of chip cards. For CVV2, where the date is keyed in from the value printed on the card, Issuers can choose to calculate the verification value in either 'YYMM' or 'MMYY' order.

The expiry date on the card provides a pointer in VEAS to the appropriate CVK with which to generate the verification value for comparison. A later expiry date may point to a more recent CVK if the Issuer has used a different one to calculate verification values for newly issued cards.

12.7.3 dynamic Card Verification Value (dCVV)

Each dCVV contactless card contains the following:

- Unique Derivation Key (UDK), the dCVV equivalent of the CVK
- PAN
- ATC
- Service code
- Expiry date

The chip on the card uses all these to calculate a dCVV. The same algorithm is used as for calculating the CVV, but the ATC and PAN are combined to produce a virtual PAN as an input to the algorithm. Since the ATC is incremented each time the card is used, the dCVV will be different for each transaction.

This dCVV is stored in the MSI and sent to VEAS (or the Issuer host) along with the:

- PAN
- ATC
- Service code
- Expiry date
- DKI (Derivation Key Index)

Issuers can use up to 256 MDKs for use on their chip cards. These will be encrypted and sent to Visa where the Issuer elects for Visa to verify the dCVV on their behalf. The DKI in the transaction indicates which MDK was used for this particular card.

The Visa Security Module uses the indicated MDK to transform the PAN to calculate the UDK on the card. It now has all the information it needs to calculate the dCVV in the same way as the chip.

The dCVV supplied in the transaction (as part of the MSI) is then verified by comparing it to the dCVV calculated by VEAS.

12.7.4 Emergency replacement cards

Through its service centres world-wide, Visa Europe is capable of producing emergency replacement cards with a valid CVV or CVV2, appropriately encoded.

Emergency replacement cards with iCVVs and dCVVs are not currently available.

12.8 Process flow

When all the requirements are met, the Card Verification Service calculates and verifies CVV, iCVV and CVV2s on transactions in the following manner.

The main authorizing steps in the Card Verification Service are:

1. CVV/iCVV/dCVV: The Acquirer transmits basic elements in the track data from the magnetic stripe or the chip's image in the magnetic stripe in the 0100 authorization request or 0200 financial request message to VEAS.
CVV2: The Acquirer transmits the basic elements (PAN, expiry date) together with the CVV2 (data field 126.1) in the 0100 authorization request or 0200 financial request message to VEAS.
2. VEAS (or the Issuer host) receives an authorization request containing relevant information, such as the service code, card number, and the expiry date.
CVV/iCVV/dCVV: Acquirers should indicate that the complete magnetic stripe is included with an appropriate value in the POS Entry Mode field (data field 22.1).
3. If VEAS performs the verification:
 - a. VEAS calculates the CVV, iCVV, dCVV and CVV2 value derived from the basic elements:
 - PAN
 - Service code
 - Expiry date
 - b. CVV/iCVV/CVV2: Encrypts using the CVK stored in the VSM.
dCVV: Encrypts using the UDK derived from the MDK stored in the VSM, together with the PAN.
 - c. Compares the CVV, iCVV, dCVV and CVV2 received in the transaction with the newly calculated value.
 - d. VEAS assigns a result code to the transaction and forwards the results to the Issuer (only if the Issuer chooses to receive the result code.).
 - e. The Issuer either accepts the VEAS verification result or performs an additional CVV, iCVV, dCVV and CVV2 value confirmation and returns the CVV, iCVV, dCVV and CVV2 result code and the appropriate response code to the Acquirer.
4. If the Issuer performs the verification:
 - a. VEAS sends the request message to the Issuer.
 - b. The Issuer calculates the CVV, iCVV, dCVV and CVV2 and returns the results and appropriate response code to the Acquirer.

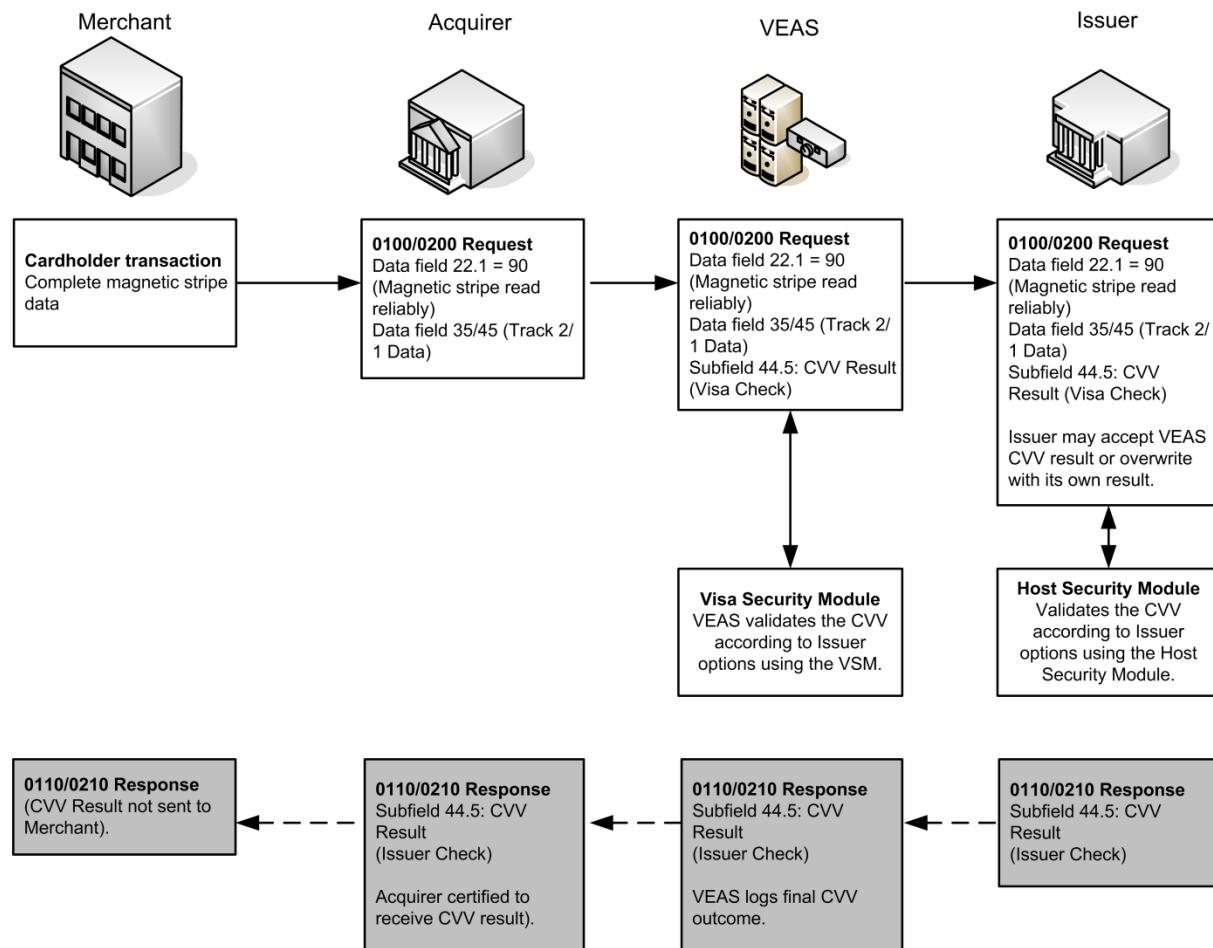
Note For CVV/iCVV/CVV2 verification requests forwarded by a VEAS Acquirer, the Acquirer must have the CVV/iCVV/CVV2 participation flag set to 'on' otherwise the transaction is downgraded. The default setting is 'on' for all Acquirers. This flag is set in data field 32 - Acquiring Institution Identification Code. See [Key data fields](#) on page 108.

12.9 Message flows

12.9.1 Card Verification Value (CVV)

The following diagram illustrates the message flow for the Card Verification Service using CVV.

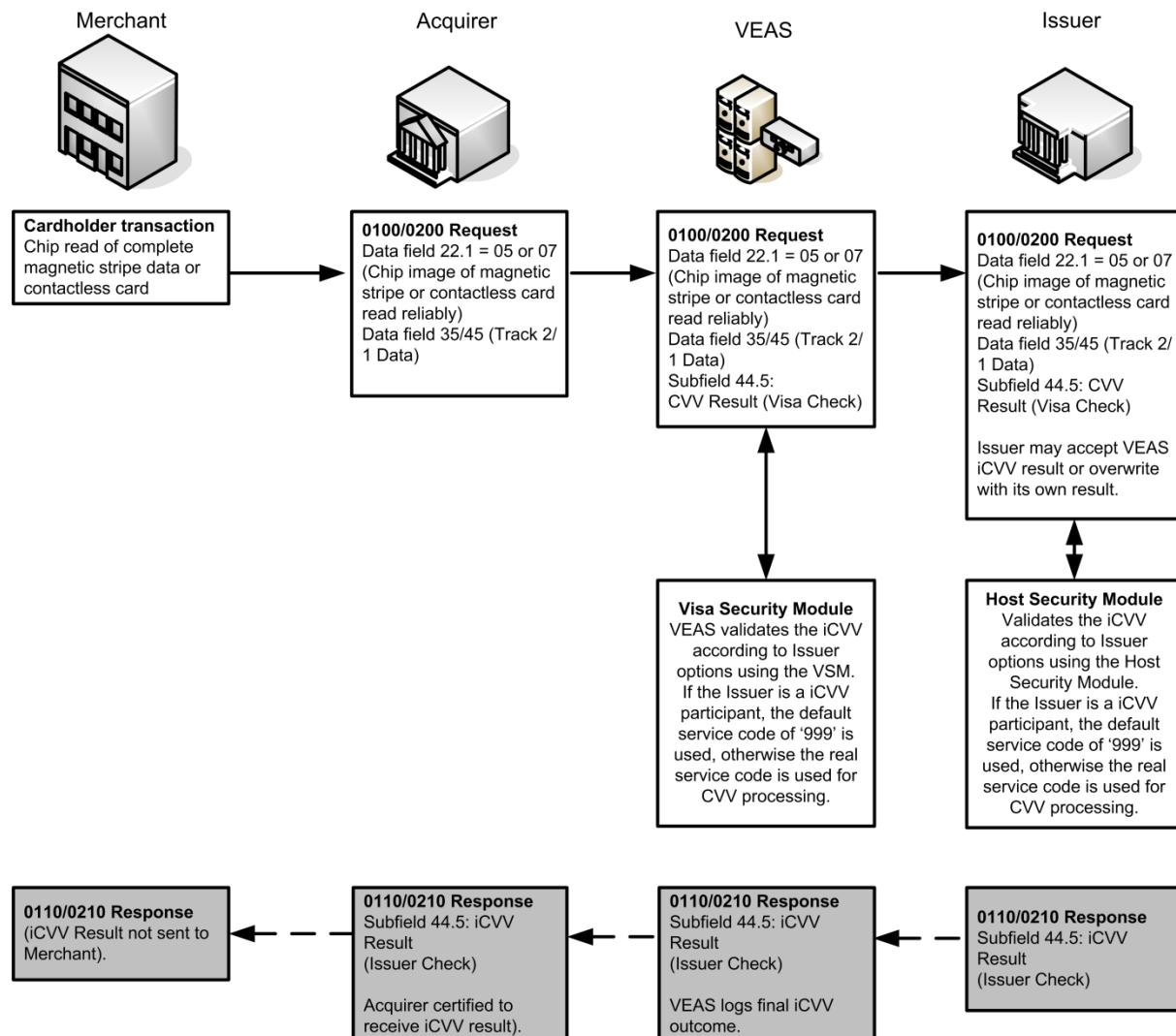
Figure 21: Message flow for the Card Verification Service using CVV



12.9.2 Integrated Chip Card Verification Value (iCVV)

The following diagram illustrates the message flow for the Card Verification Service using iCVV.

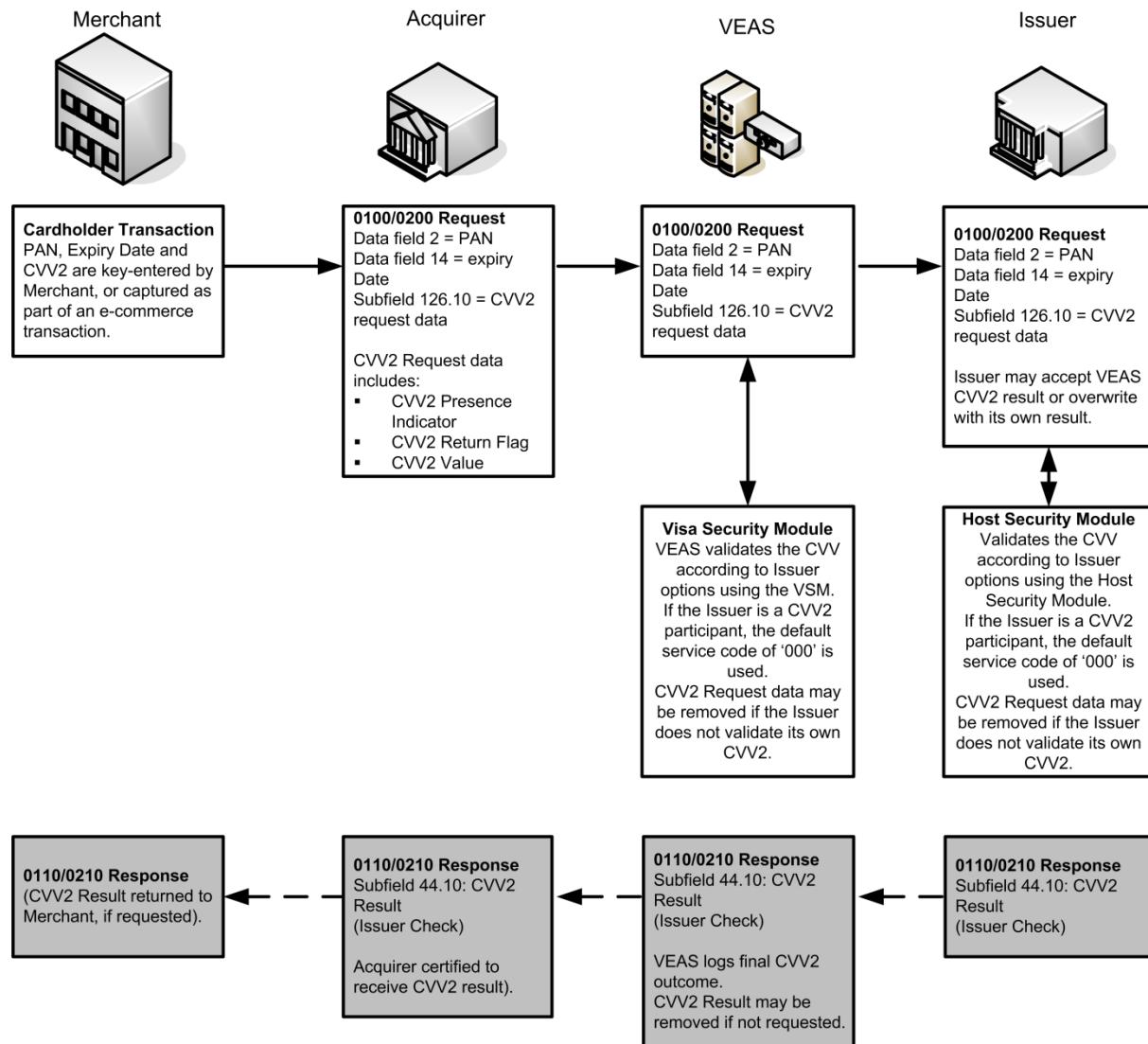
Figure 22: Message flow for the Card Verification Service using iCVV



12.9.3 Card Verification Value 2 (CVV2)

The following diagram illustrates the message flow for the Card Verification Service using CVV2.

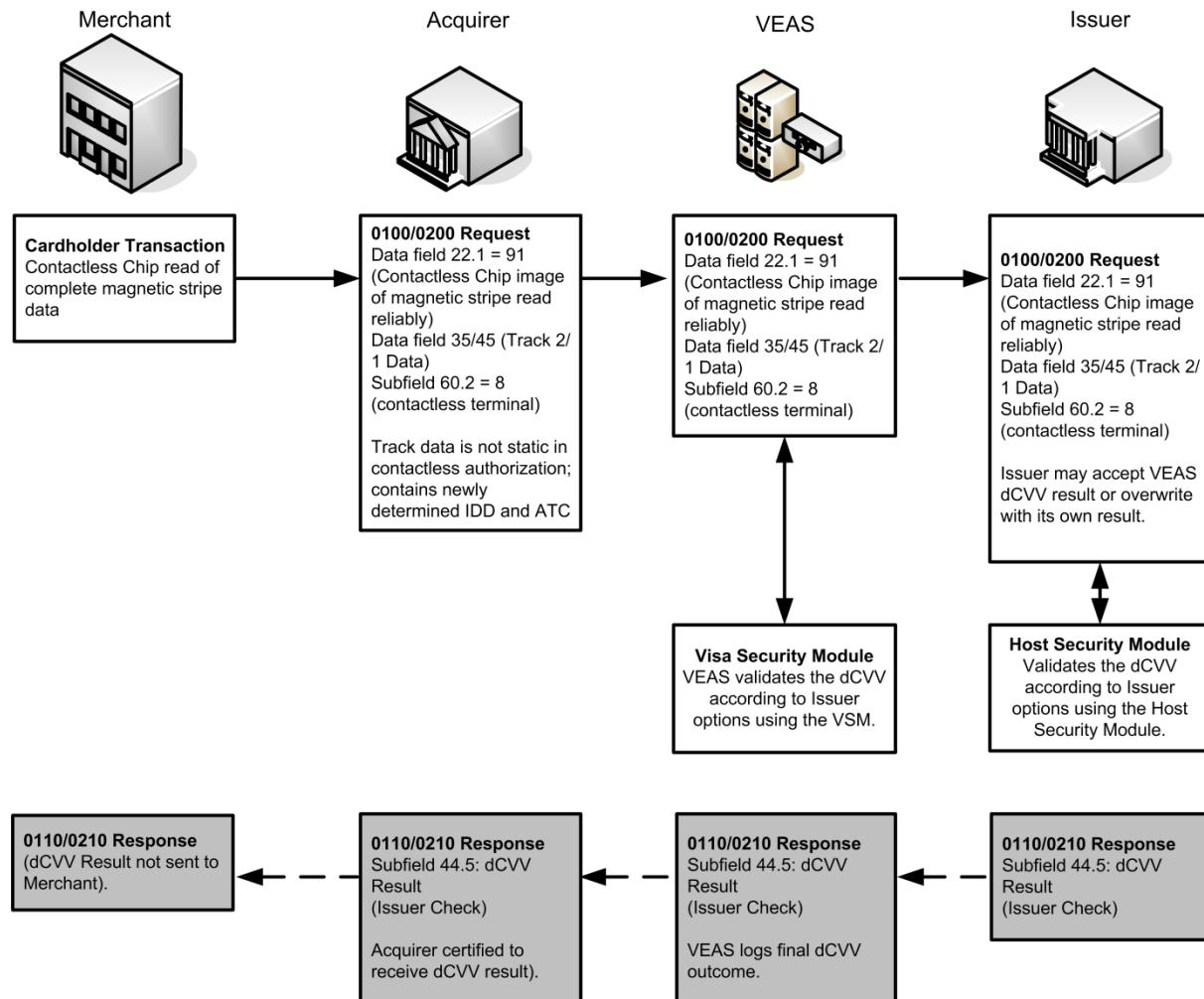
Figure 23: Message flow for the Card Verification Service using CVV2



12.9.4 Dynamic Card Verification Value (dCVV)

The following diagram illustrates the message flow for the Card Verification Service using dCVV.

Figure 24: Message flow for the Card Verification Service using dCVV



Important The Acquirer must send the correct POS Entry Mode Code (data field 22), MSI (data field 35/45) and Terminal Type (data field 60.2).

12.10 Key messages

The following message types carry CVV, iCVV, dCVV and CVV2 data when using the Card Verification Service:

- 0100 authorization request
- 0200 financial request

The following message types carry CVV, iCVV, dCVV and CVV2 result data:

- 0100 authorization request
- 0200 financial request
- 0110 authorization response

- 0120 authorization stand-in advice
- 0210 financial response
- 0220 financial stand-in advice

12.11 Key data fields

The following key data fields are used by the Card Verification Service. For detailed information about each data field, see the Visa Europe technical specifications.

Data field 14 - Date, Expiry (CVV2)

This data field must contain the expiry date of the card for use in the card verification process. The expiry date determines which encryption key to use.

Data field 22.1 - POS Entry Mode

This data field contains the POS Entry Mode. It determines whether the track data is from the magnetic stripe, chip or contactless card.

Data field 32 - Acquiring Institution Identification Code (request message)

This data field contains the Acquirer Institution Identification Code. Acquirers must be certified for CVV/iCVV.

Data field 35 - Track 2 Data

This data field (or data field 45) contains the track data from the magnetic stripe, or Magnetic Stripe Image if a qVSDC chip card is used.

For more information about the format specifications for Track 2, see the *Payment Technology Standards Manual*.

Data field 44 - Additional Response Data

This field contains miscellaneous response message data (although it may contain some in a request if VEAS has performed some work).

Data field 45 - Track 1 Data

This data field (or data field 35) contains the track data from the magnetic stripe or chip if a qVSDC chip card is used.

For more information about format specifications for Track 1 see the *Payment Technology Standards Manual*.

Data field 60.2 - Terminal Entry Capability

Data field 60-Additional POS Information, contains a subfield with the Terminal Entry Capability.

Data field 126 - Visa Private-Use Fields (CVV2)

This data field has been renamed from field 126 - Electronic Banking Fields to Visa Private-Use Fields by Visa Europe. It is defined in bit-mapped field format.

13 Chargeback Reduction Service

Chargebacks are transactions that Issuers return to Acquirers through the Visa Europe System. A chargeback is raised when a presentment is disputed by the Cardholder.

CRS performs checks on presentments and chargebacks, and returns certain invalid items to the Acquirer or Issuer, as appropriate. This reduces Member costs associated with dispute processing.

13.1 Acquirer benefits

CRS adds information to the messages that are received by Acquirers from Issuers and validates chargebacks.

The service automatically returns some invalid, authorization-related chargebacks to Issuers on behalf of Acquirers. This reduces the amount of research and processing time that Acquirers need to address or remedy chargebacks.

13.2 Issuer benefits

CRS adds data to the messages that are received by Issuers from Acquirers.

Issuers are able to review the data returned by CRS and follow the correct dispute resolution process, making better-informed chargeback decisions, with lower research costs.

The service automatically returns some invalid, authorization-related transactions to Acquirers on behalf of Issuers, thus eliminating the Issuer's research and processing time for these transactions.

13.3 Participation

The CRS is available through VECSS. All Members automatically participate in the service.

Note For SMS Members, CRS is used for Visa (and Electron) POS transactions only.

13.4 Related information

For further information about the CRS, see the following documents:

- *Dual Message System Clearing (DMSC) Reports*
- *Dual Message System Clearing (DMSC) Technical Specifications*
- *Visa Europe Merchant Data Standards Manual*

To arrange implementation of CRS, contact Visa Europe Customer Support.

13.5 How the service works

The procedure for validating transactions varies slightly, depending on whether CRS is used by:

- An Acquirer to validate original transactions, or
- An Issuer to validate chargebacks

13.5.1 Validating POS transactions

For Acquirers, the main steps in the CRS are:

1. The Acquirer enters original purchase or cash transactions into Interchange at the Processing Centre of the Acquirer. The outgoing Interchange is sent to the Visa Interchange Center (VIC).
2. At the VIC, CRS evaluates transactions and inserts status indicators for the validation process. Availability of this data helps Acquirers to manage any disputes that may arise.
3. The destination of the transactions depends on whether or not CRS validates them.
 - Valid transactions are sent to the Issuer.
 - Invalid transactions are returned to the Acquirer when all of the following conditions are met:
 - The account number is listed in the Card Recovery Bulletin (CRB) as of 04:00 GMT on the date before the transaction takes place
 - The Transaction Amount is equal to or below the floor limit of the Merchant
 - No authorization code is present

13.5.2 Validating chargebacks

For Issuers, the main steps in the CRS are:

1. Chargebacks pass through a first stage of CRS validation during outgoing Edit Package processing at the Processing Centre of the Issuer. This ensures that they meet certain processing requirements.

Their destination depends on whether or not CRS validates them:

- Validated chargebacks are sent to the VIC as outgoing Interchange.
 - If a chargeback fails to meet the processing requirements, it is rejected and it is prevented from entering into VECSS Interchange. The Issuer must resolve the problem before the transaction can be a part of outgoing Interchange.
2. At the VIC, CRS further evaluates chargebacks and inserts status indicators for the validation process.

Their destination depends on whether or not CRS validates them:

- CRS forwards valid chargebacks to the Acquirer
- CRS returns invalid chargebacks to the Issuer

chargebacks that are returned to the Issuer by the CRS appear in the Edit Package Chargeback Reduction Service - Returned Item Report series.

13.5.2.1 Edit Package validation of chargebacks

Edit Package rejects chargebacks in the following cases.

Table 10: Reasons Edit Package rejects a chargeback

Reason	Explanation	Applicable to
No Member message text	Chargebacks are rejected if there is nothing in the Member message text field. For further information, see the applicable payment scheme or processing rules and the <i>DMSC Technical Specifications</i> .	Transactions with certain Travel and Entertainment (T&E) chargeback reason codes
Incompatible chargeback reason codes	Chargebacks that do not have a reason code compatible with the transaction's Merchant Category Code are rejected. For example, an international ATM Transaction cannot be returned to the Issuer with a chargeback reason code 75 (inadequate message content).	Express Payment Service (EPS), automatic teller machine (ATM) and T&E transactions
Number of presentations exceeded	Edit Package rejects chargebacks if the permitted number of chargebacks has been exceeded: <ul style="list-style-type: none"> ■ Acquirers are limited to one presentation and one Representation ■ Issuers are limited to one chargeback 	All further chargebacks after the limits have been reached

13.5.2.2 Visa Interchange Center validation of chargebacks

In addition to validation through outgoing Edit Package processing at the Processing Centre of a Member, chargeback transactions are analysed again during processing at the VIC for authorization-related data. CRS returns invalid chargebacks to Issuers under the following conditions.

Table 11: Conditions under which CRS returns invalid chargebacks to Issuers

Chargeback reason code	Meaning	Explanation
72	No Authorization	<p>Where either of the following conditions apply:</p> <ul style="list-style-type: none"> ■ The transaction was above the floor limit of the Merchant, but the chargeback reason code indicated that the transaction was below the floor limit; or ■ The reason code indicated that the transaction exceeds the floor limit when the transaction amount is actually under the floor limit of the Merchant. <p>CRS allows a plus or minus 20% tolerance level, above or below the floor limit, before returning the transaction.</p>
70	Card Recovery Bulletin or Exception File	<p>The account number was not listed in the CRB or Exception File for the Merchant's region on the date of the transaction, but the chargeback reason code indicates that it was listed.</p> <p>This is based on the CRB/Exception File history file that is maintained at each VIC.</p>
Invalid		A chargeback of an ATM Transaction contained an invalid reason code.

13.5.3 Adding status indicators

CRS adds the following status indicators to records whenever specific conditions exist:

- Floor limit indicator
- CRB/Exception File indicator
- PCAS indicator

CRS validation does not take place if any data element needed to determine the status of the floor limit, card pickup bulletin or authorization code is missing from the transaction. In this case, DMSC applies the 'validation not performed or insufficient information' indicator code to the transaction.

Note The floor limit, Card Recovery Bulletin (CRB)/Exception file and Positive Cardholder Authorization Service (PCAS) indicators' edits apply only to original POS transactions, not their representents.

13.5.3.1 Floor limit indicator

CRS adds a floor limit indicator if the transaction was above or below the floor limit of the Merchant for the date of the purchase according to the applicable payment scheme or processing rules.

CRS validates the following transaction elements to determine the floor limit:

- Account type
- Mail/telephone indicator

- Merchant location
- Merchant Category Code
- Reimbursement fee category
- Special condition indicator
- Chip/non-chip
- Transaction Date

When the transaction is validated at the VIC, the VIC inserts the appropriate code in TCR 0, field position 24, Floor Limit Indicator.

13.5.3.2 CRB/Exception File indicator

CRS adds a CRB/Exception File indicator if the account number on the card used in the transaction was listed in the CRB for the Merchant's region on the date of the transaction.

CRS evaluates the following transaction elements to determine the account status on the card pickup bulletin:

- Account number
- Mail/telephone indicator
- Merchant location
- Transaction Date
- Authorization code
- Floor limit indicator

When the transaction is validated at the VIC, the VIC inserts the appropriate code in TCR 0, field position 25, CRB/Exception File Indicator.

13.5.3.3 PCAS indicator

CRS adds a PCAS indicator if the transaction's authorization code was generated during stand-in authorization (STIP: stand-in processing) using the PCAS.

CRS evaluates the following elements to determine the authorization status:

- Account number
- Authorization code
- Transaction Date

When the transaction is validated at the VIC, the VIC inserts the appropriate code in TCR 0, field position 26, PCAS Indicator.

13.5.4 Advice messages and reports

Chargebacks returned to the Issuer by the CRS appear on the Edit Package Chargeback Reduction Service–Returned Item Report series:

- EP-206A: Chargeback Reduction Service - Returned Item Detail
- EP-206B: Chargeback Reduction Service - Returned Item Summary by BIN
- EP-206C: Chargeback Reduction Service - Returned Item Summary by Centre

Visa Europe also provides related additional monthly reports.

13.5.4.1 EP-206A: CRS - Returned Item Detail

This report contains a formatted image of the returned transaction along with the return reason code. The reporting sequence is:

1. BIN
2. Return reason code
3. Transaction code

Along with the original transaction, the original batch date, transaction code, batch number, the item within the batch and the return reason code are given.

13.5.4.2 EP-206B: CRS - Returned Item Summary by BIN

This report summarises by BIN the transactions that are returned by the VIC to the Processing Centre. The reporting sequence is:

1. BIN
2. Return reason code
3. Transaction code
4. Transaction Currency

13.5.4.3 EP-206C: CRS - Returned Item Summary by Centre

This report summarises by Processing Centre the transactions that are returned by the VIC. The reporting sequence is:

1. Return reason code
2. Transaction code
3. Transaction Currency

13.5.4.4 Additional monthly reports

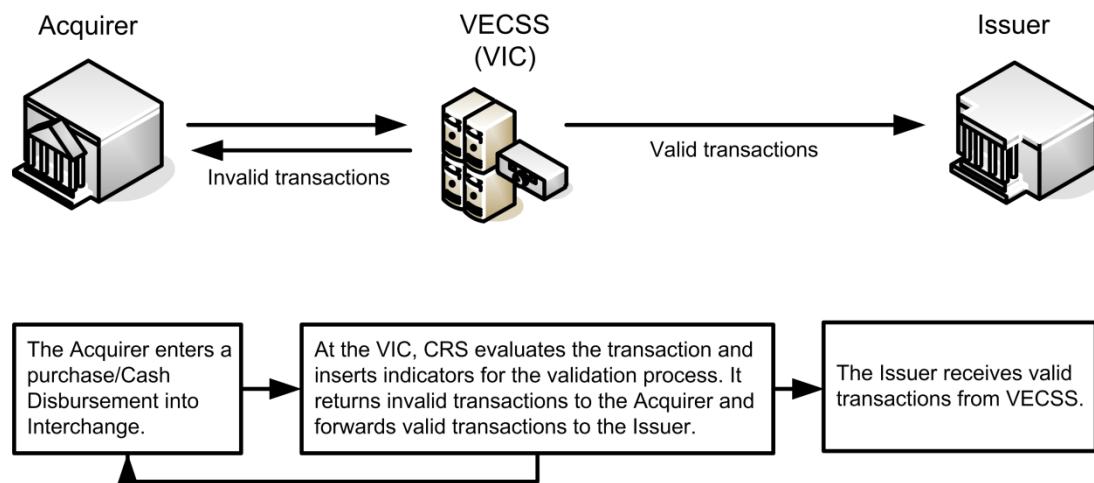
In addition to the EP-206A, EP-206B and EP-206C reports, three additional reports are provided by Visa Europe on a monthly basis:

- CBRMR201-A: Chargeback Reduction Service Detail
- CBRMR301-A: Chargeback Reduction Draft (Issuer) Detail
- CBRMR302-A: Chargeback Reduction Draft (Acquirer) Detail

13.6 Process flows

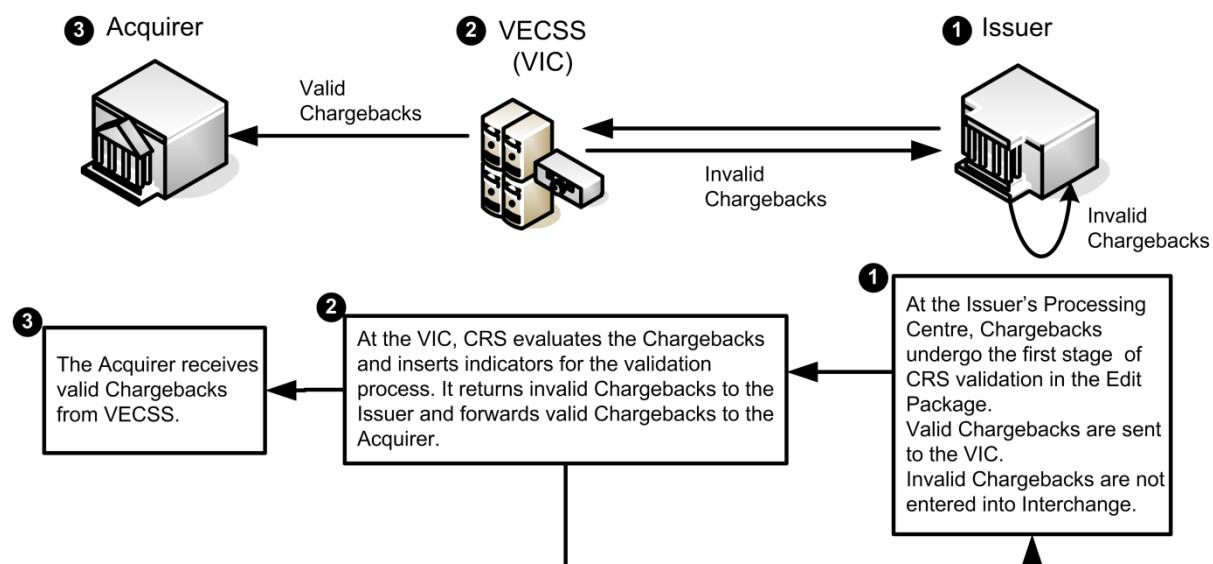
The following diagram illustrates the process flow for Acquirers using the CRS.

Figure 25: Process flow for Acquirers using the CRS



The following diagram illustrates the process flow for Issuers using CRS.

Figure 26: Process flow for Issuers using the CRS



14 Cross-Border Domestic Interchange Program

The Visa Europe Cross-Border Domestic Interchange Program (Cross-Border Domestic Interchange Program) enables participating Members to choose to pay fixed, multilaterally-agreed interchange fees (MIFs) on cross-border acquired transactions where:

- The Merchant Outlet is based in the European Economic Area (EEA)
- The Merchant Agreement sets the Merchant Service Charge on a MIF Plus Plus basis.
For information about MIF Plus Plus, see the *Cross-Border Domestic Interchange Programme Merchant Registration Guide*
- Transactions are processed securely
- Transactions are identified with a Single Merchant Identifier (SMI)
- Transactions are consumer transactions

MIFs for cross-border acquired transactions that qualify for the service are capped by the European Commission at the following rates:

- 0.2% - debit cards
- 0.3% - credit cards

Note A German Domestic Secure Interchange Plus Plus fee program also exists. This program has identical procedures and processes to those of the Cross-Border Domestic Interchange Program. Acquirers of German Merchants can register Merchants in either program.

14.1 Related information

For further information about the Cross-Border Domestic Interchange Program, see the following document:

- *Cross-Border Domestic Interchange Programme Merchant Registration Guide*

14.2 Participation

Participation is optional for Acquirers.

Acquirers that choose to participate in the program must meet the conditions set out in the applicable payment scheme or processing rules.

Participating Acquirers must have an active Visa Online (VOL) subscription. They must register their Merchant Agreements and Merchant Outlet details with Visa Europe through VOL. For more information, see the *Cross-Border Domestic Interchange Programme Merchant Registration Guide*.

14.2.1 Testing

Testing is optional for the Cross-Border Domestic Interchange Program. To arrange for testing, Members should contact Visa Europe Customer Support.

14.3 How the service works

The Cross-Border Domestic Interchange Program has two functions:

- Registration of Merchants on VOL
- Identification of qualifying transactions during Visa Europe Clearing and Settlement Service (VECSS) processing

14.3.1 Registering Merchants on VOL

Participating Acquirers register qualifying Merchants with Visa Europe using the Cross-Border Domestic Interchange Program application on VOL. For each Merchant that they register, Acquirers must provide information proving that their Merchant Agreement is based on unblended MIF Plus Plus pricing.

For each Merchant that is successfully registered, Visa Europe provides the Acquirer with a Single Merchant Identifier (SMI). The SMI is required for the Acquirers to claim the fixed MIFs for transactions that have been processed through the program.

For more detailed information about Merchant registration and additional functions of the Cross-Border Domestic Interchange Program application on VOL, see the *Cross-Border Domestic Interchange Programme Merchant Registration Guide*.

14.3.2 VECSS processing

To qualify for the Cross-Border Domestic Interchange Program MIFs, VECSS assesses transactions to ensure they meet the following conditions:

- The transaction has a valid SMI
- The Fee Program Indicator is set to 5CB
- The transaction's Card Acceptor ID is valid for the Acquirer and the SMI combination
- The transaction is a POS transaction on a consumer card
- The Merchant is within the EEA and the Acquirer is within the Europe region
- The Acquirer and the Merchant are in different countries
- The transaction is a Domestic Transaction
- The transaction is secure, that is to say, has been correctly accepted by the Merchant using EMV, Verified by Visa or other equivalent secure Visa Europe technology

Members that participate in the program will be able to identify transactions that qualify for the Cross-Border Domestic Interchange Program fees through fee descriptors in their Visa Europe Settlement Service (VSS) reports. For a complete list of these fee descriptors, see the *DMSC Technical Specifications*.

14.4 Process flow

This section provides a high-level overview of the process flow for the Cross-Border Domestic Interchange Program.

1. Acquirer registers a qualifying Merchant on to the program.
2. Visa Europe provides an SMI to the Acquirer.
3. Acquirer ensures that the authorization message for a cross-border acquired transaction contains the:
 - SMI
 - Fee Program Indicator (FPI) specific to the program
 - Card Acceptor ID

Note This information is contained in the authorization message in Single Message System (SMS) processing. For Dual Message System Authorization (DMSA), the information is sent as part of the clearing message.

4. VECSS assesses the transaction to ensure it meets all conditions to qualify for Cross-Border Domestic Interchange Program fees (see [VECSS processing](#) on the previous page).
5. For qualifying transactions, VECSS assesses the transaction to determine the applicable MIF, which is dictated by the account funding type source of the transaction.
6. VECSS calculates the settlement position for the transaction.

The settlement position is provided in VSS reports.

14.5 Key messages

14.5.1 Authorization

The following are the key authorization messages for the Cross-Border Domestic Interchange Program:

- 0200/0210 - Full financial request/full financial request response
- 0220/0230 - Representment/representment
- 0282/0292 - Representment status advice/representment status advice response
- 0400/0410 - Reversal/reversal response
- 0420/0430 - Reversal advice/reversal response
- 0422/0432 - Chargeback/chargeback response
- 0480/0490 - Chargeback status advice/chargeback status advice response

14.5.2 Clearing

The following are the key Clearing records for the Cross-Border Domestic Interchange Program:

- TC 05, TCR 1, positions 111-127
Contains the SMI.
- TC 05, TCR 6, positions 76-78
Contains the Fee Program Indicator. For the Cross-Border Domestic Interchange Program, this must be 5CB.
- TC 04, TCR 9, positions 72-87 and 88-103
Contains the Fee Descriptor.

14.6 Key data fields

The following key data fields are used by the Cross-Border Domestic Interchange Program. For detailed information, see the Visa Europe technical specifications.

Data field 42 - Card Acceptor Identification Code

This data field contains an alphanumeric code that identifies the card acceptor operating the point-of-sale or point-of-service terminal in both local and Interchange environments. The value in this field must be identical to the value submitted during Merchant registration.

Data field 63.19 - Fee Program Indicator

This data field contains an Interchange Reimbursement Fee program indicator (FPI). For the Cross-Border Domestic Interchange Program, the value is 5CB.

Data field 104, Usage 1 - Transaction Description

This data field contains transaction-specific datasets presented in hex number order. For the Cross-Border Domestic Interchange Program, the field contains the SMI.

15 Currency Conversion Service

The Currency Conversion Service relates to dual message processing in the Visa Europe Clearing and Settlement Service (VECSS).

For information about currency conversion for dual message processing in the Visa Europe Authorization Service (VEAS) and in Single Message System (SMS) processing, see [Multicurrency Service](#) on page 174.

The Transaction Amount in destination currency (TADC) is the amount that is calculated for each transaction and is posted to the Cardholder's account.

Note The TADC may differ from the Settlement Amount due to the choice of Settlement Currency, Interchange fees, and other variables.

The Currency Conversion Service enables Members to clear transactions in most currencies that are recognised by the International Organization for Standardization (ISO) and supports settlement in a number of international currencies (for an up-to-date list of international currencies, contact Visa Europe Customer Support).

The Currency Conversion Service includes the following Transaction Currency processing features:

- **Clearing conversion:** Automatically converts the Transaction Currency to the Billing Currency. The Transaction Currency is generally the currency in which a transaction takes place. The Billing Currency is the currency in which the Cardholder receives their bill (usually the country in which the account is domiciled). The Visa Europe System supports most currencies that are recognised by the ISO.
- **Settlement conversion:** Automatically converts the Transaction Currency to the Acquirer's Settlement Currency (if the two are different) and to the Issuer's Settlement Currency (if the two are different). The Currency Conversion Service supports a number of Settlement Currencies.

Members can also subscribe to several related optional services:

- **Currency Rate Delivery Service:** Provides Members (five days a week, Tuesday to Saturday) with the Currency Conversion Rates (in TC 56 format) that Visa Europe uses to process transactions.
For more information, see [Currency Rate Delivery Service](#) on page 188.
- **Enhanced Interchange Data Service:** Participating Issuers automatically receive the Interchange Reimbursement Fee amounts and applicable Currency Conversion Rate in each clearing transaction sent to them by the Visa Europe Clearing and Settlement Service (VECSS).
For more information, see [Enhanced Interchange Data Service](#) on page 130.

15.1 Related information

For further information about the Currency Conversion Service, see the following documents:

- *Dual Message System Clearing (DMSC) Technical Specifications*
- *Dual Message System Authorization (DMSA) Technical Specifications*

For further information about Settlement Currencies, including a list of those offered by Visa Europe, see the following document:

- *Visa Europe Settlement Funds Transfer Guide*

15.2 Participation

The Currency Conversion Service is available through VECSS to users of dual message processing.

Participation is mandatory for Members.

15.3 How the service works

The main steps in the Currency Conversion Service are:

1. The Acquirer submits the transaction to the Visa Europe System in the currency in which the transaction is completed.
2. The Visa Europe System performs standard clearing and currency conversion. For information about how currency is converted, see *How currency conversions are calculated* on page 178.

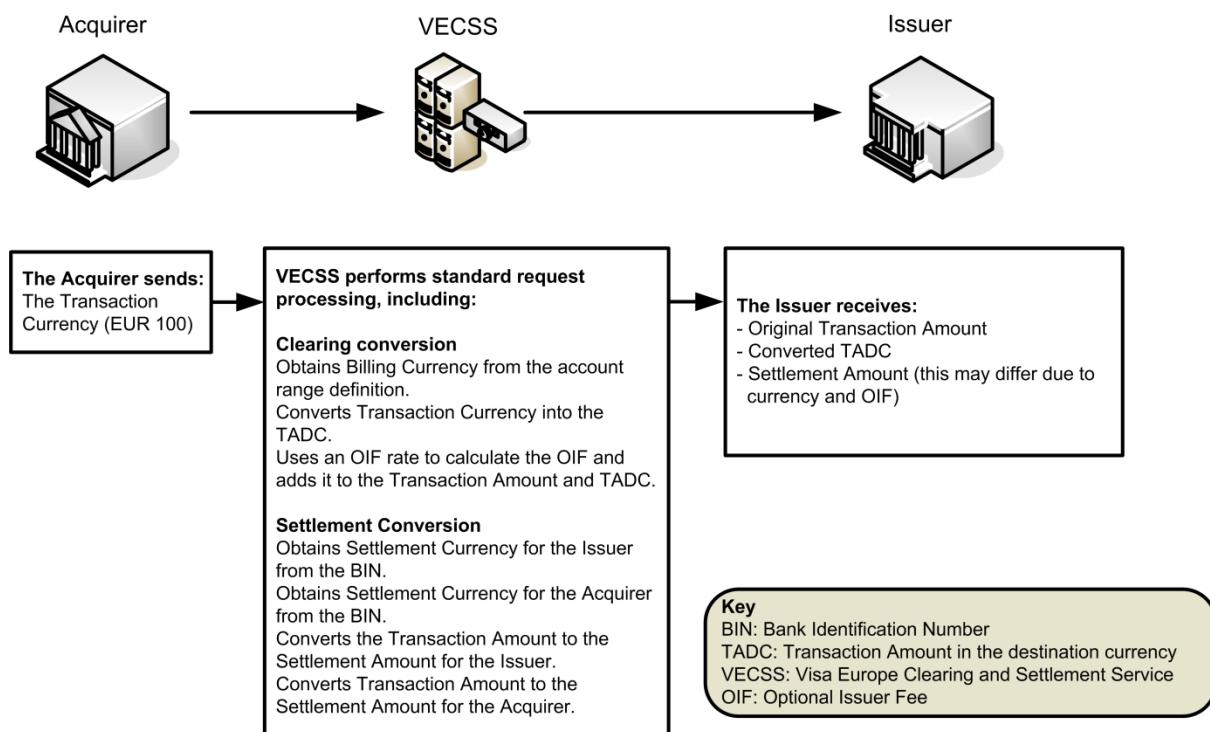
For transactions that require currency conversion, Issuers can choose to charge a fee, known as the Optional Issuer Fee, to the Cardholder. If they choose to do this, this fee is included in the transaction Destination Amount field. For more information, see *Charging an Optional Issuer Fee* on page 178.

3. The Visa Europe System routes the transaction to the Issuer. Both the Acquirer and Issuer can choose to settle in any supported Settlement Currency. For more information, see *Choosing the Settlement Currency* on page 124.

Issuers can also choose to:

- Receive information about Currency Conversion Rates. For information, see *Currency Rate Delivery Service* on page 188.
- Receive the Interchange Reimbursement Fee amount and Currency Conversion Rates used in each clearing transaction. For more information, see *Enhanced Interchange Data Service* on page 130.

The following diagram illustrates the process flow for converting the currency of a UK Cardholder transaction that is to be acquired in euros.

Figure 27: Clearing and settling a multicurrency transaction

Note The Optional Issuer Fee (OIF) is not included in the Settlement Amount but is just added to the TADC. For an explanation of TADC and other terms relating to currency conversion, see [Understanding rate-related terminology](#) on page 125.

15.3.1 Understanding decimal positioning

Currencies are defined as having zero, two or three minor units of currency. For example, the euro has two minor units of currency (the two positions to the right of the decimal point); the Japanese yen has no minor units. VECSS always assumes two minor units.

For a list of countries, currencies and their minor units, see *Dual Message System Authorization (DMSA) Technical Specifications*.

The following table gives examples of decimal positioning.

Table 12: Examples of decimal positioning

If the transaction amount is	And the number of minor units of currency is	It is entered in the transaction or request message as
20492	2	2049200
67.89	2	6789
3.129	2	313
500000	0	50000000

Note Some fields have specific formats, for example, they require leading zeros. For more information, see the *Dual Message System Authorization (DMSA) Technical Specifications*.

15.3.2 How currency conversions are calculated

The Visa Europe System uses two components to convert currencies:

- A buy and/or sell rate to obtain the TADC
- The OIF, if any, for presentments of original transactions

The sum of TADC and Optional Issuer Fee is carried in the Destination Amount field.

15.3.2.1 Currency conversion rate pairs

Visa Europe uses buy and sell rates determined from rates available on currency markets for currency conversion. These rates are paired into:

- USD-based rates that are used when converting non-USD currencies against the US dollar.
- Cross rates (non-USD-based rates) that are used for selected currencies for which the rates quoted are against a currency other than the US dollar. The cross rates that the Visa Europe System uses are available on request.

15.3.3 Charging an Optional Issuer Fee

Issuers can choose to charge an Optional Issuer Fee (OIF), which is a percentage rate established by the Issuer, to the Cardholder for transactions that require currency conversion. The Issuer can specify a Visa Europe OIF or international OIF, or both fees.

The OIF, which may be positive or negative, is maintained in the Visa Europe System databases according to the Issuer's BINs or account range. OIFs applied at the account range level take precedence over those applied at the BIN level. This optional fee is calculated at conversion time, using the percentage rate established by the Issuer. It is included in the transaction's Destination Amount field. To modify an existing OIF, contact Visa Europe Customer Support.

Note The OIF is not included in the Settlement Amount but is added to the TADC.

All Visa Europe systems that support the Currency Conversion Service use common Currency Conversion Rates.

15.3.4 Choosing the Settlement Currency

The service automatically converts your net financial position into any of the currencies supported by the International Settlement Service. You can choose to settle in any of the supported Settlement Currencies. For information on supported Settlement Currencies, see the *Visa Europe Settlement Funds Transfer Guide*.

15.4 How buy and sell currency rates are applied to transactions

This section describes how the Visa Europe Clearing and Settlement Service (VECSS) applies buy and sell rates to transactions during clearing and settlement.

15.4.1 Understanding rate-related terminology

Visa Europe's Currency Conversion Rate system involves specific terminology as defined in the following table.

Table 13: Rate-related terminology

Term	Description
Base currency	Variable units of a base currency are equivalent to one unit of a counter currency
Counter currency	One unit of a counter currency is equivalent to variable units of a base currency
Buy rate	The number of units of base currency required to buy one unit of the counter currency
Sell rate	The number of units of base currency received from selling one unit of the counter currency
Source amount	The purchase value in Transaction Currency
USD-based rate pair	A rate pair in which the US dollar is always the base currency. The rate expresses a variable number of US dollars for each unit of the counter currency. The counter currency is a currency other than USD.
Non-USD-based rate (cross rate) pair	A rate pair in which the rate quoted is between two currencies, neither of which is the US dollar. Such rates are applied only when the currencies of the cross rate pair are the only currencies between the source amount and the TADC. Rates are expressed as a variable amount of base currency per unit of counter currency.
Triangulation	Triangulation occurs when no cross rate exists between a non-USD-based rate pair. In this situation the source amount is converted into USD and then the USD is converted into the TADC.
Exchange direction	The set of currency conversion calculations that are applied to a transaction, based on the transaction type
Transaction Amount in destination currency (TADC)	The submitted Transaction Amount in the currency that is appropriate to the destination endpoint. The TADC is included in the Destination Amount field. In addition to the TADC, the Destination Amount field may contain the OIF (see Charging an Optional Issuer Fee on the previous page). The Destination Amount field is provided in clearing transactions to the destination Member. Issuers have the discretion to increase or decrease the amount in this data field when billing Cardholders.

The following table provides a mapping of the terminology used in the above table with the corresponding fields in a DMSC message, as described in the *Dual Message System Clearing (DMSC) Technical Specifications* manual.

Table 14: Rate-related terminology mapped to fields in DMSC message

Term	DMSC TCR/Position
Source amount	Draft Data TCR 0, Positions 77-88
TADC (in Destination Amount data field)	Draft Data TCR 0, Positions 62-73 In the <i>Dual Message System Clearing (DMSC) Technical Specifications</i> manual, only the TADC component is described and displayed in these data fields. The OIF and currency conversion fee are not addressed.

15.4.2 How rate pairs are determined

When converting currencies, the Visa Europe System compares the source currency and the destination currency to determine whether to use a USD-based or a non-USD-based rate pair for a transaction.

The Visa Europe System applies the USD-based rates to all settlement services and to all amounts, including assessments and charges that are displayed in daily settlement reports, except when **all** of the following conditions are met. In this case, a non-USD-based rate is applied:

- The source amount and the TADC are in different non-USD currencies and a non-USD-based rate pair exists
- A non-USD-based rate pair (for example, euros to pounds sterling) was used to calculate the TADC
- A non-USD-based rate exists that matches the currencies of the source amount and the specified Settlement Amount, either source Settlement Amount or destination Settlement Amount

The Visa Europe System applies USD-based rates to transactions when a match between the currencies in the transaction and a corresponding non-USD-based rate pair is not found on the Rate File (the currency rates file distributed by Visa Europe to Members on request).

15.4.3 How buy and sell rates are applied

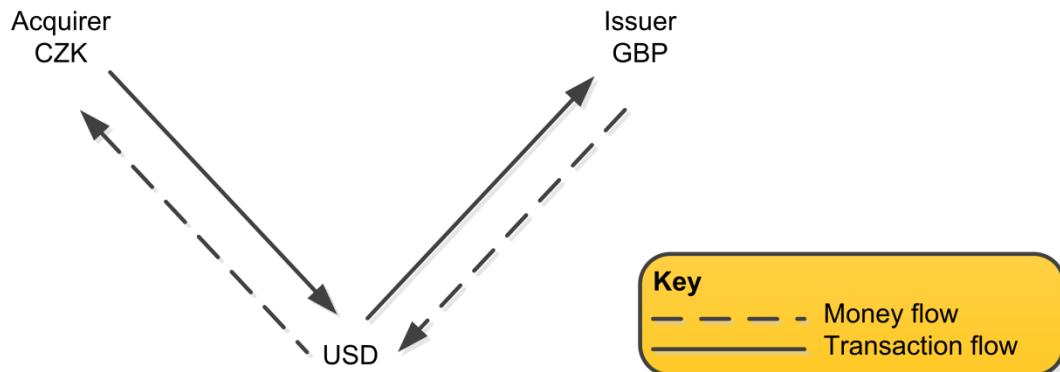
After the Visa Europe System has established the rate pairing type (see *How rate pairs are determined* on page 181) it determines which rate (buy or sell) within the pair to apply to the transaction, based on what is happening to the counter currency. If more than one conversion is required, both a buy rate and a sell rate can be applied in the same transaction. This is the case when converting between currencies for which no direct exchange rate is available. Under these circumstances, US dollars (USD) are used for conversion.

For example, for a transaction where a UK Cardholder uses their card in the Czech Republic, pounds sterling (GBP) must be converted to Czech koruna (CZK). As there is no direct exchange rate, Visa Europe sells the GBP and buys USD, then sells USD and buys CZK.

Note Although the transaction flow is from Acquirer to Issuer, the money flows from Issuer to Acquirer.

The process of converting from one currency to another via a third currency is known as triangulation. In the following scenario, the transaction flow is from Acquirer to Issuer.

Figure 28: Triangulation - Acquirer to Issuer



The following are the basic formulae that the Visa Europe System uses for all transactions when converting currencies.

Table 15: Formulae for converting currencies

When converting from	The formula is
Counter currency to base currency	Amount in counter currency x rate = Amount in base currency
Base currency to counter currency	Amount in base currency ÷ rate = Amount in counter currency

From these basic formulae, Visa Europe has established calculations for each type of transaction and has categorised them into the following exchange direction groupings:

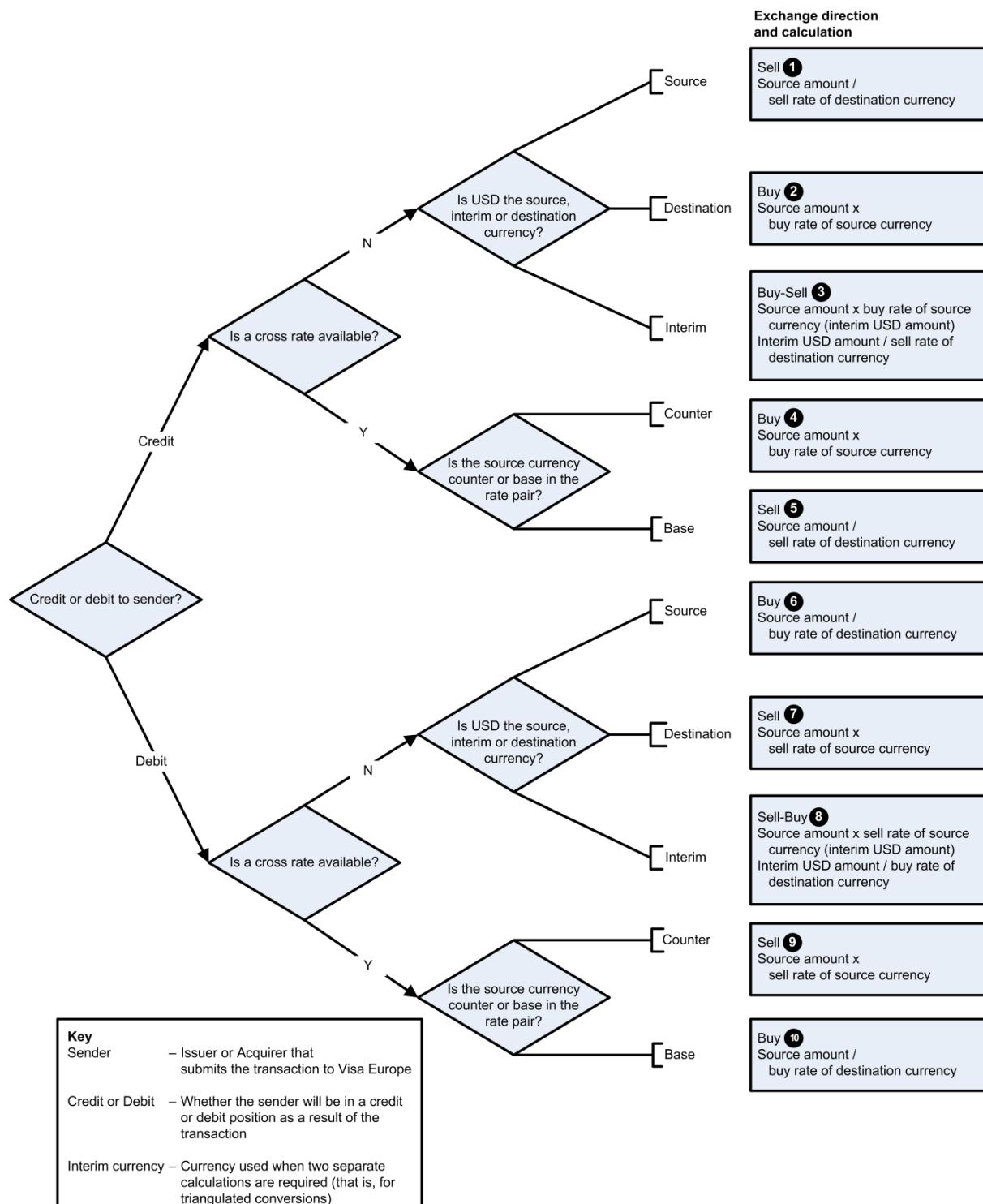
- **Buy:** Used when a cross rate is involved or where USD are the source or destination
- **Sell:** Used when a cross rate is involved or where USD are the source or destination
- **Buy-Sell:** Used when a triangulated rate is involved
- **Sell-Buy:** Used when a triangulated rate is involved

The Visa Europe System uses exchange direction calculations for the rate pair type that is appropriate for the transaction and for the type of conversion that is required when converting currency. For a brief summary of how Visa Europe converts currency, with examples, see [Currency conversion process in brief](#) below.

15.5 Currency conversion process in brief

The following decision tree shows how the Visa Europe System determines the type of conversion that is required to convert a source amount to a TADC.

Figure 29: Conversion of source amount to TADC



Note This diagram refers to the rates applied in TC 56 reports.

15.6 Examples of currency conversions

The following table shows examples of each of the preceding calculations applied to currency rate conversions. The **No.** column indicates the relevant calculation from [Figure 29](#).

Table 16: Examples of currency conversions

No.	Source currency	Source amount	Destination currency	Rate pair(s)	Rates (Buy/Sell)	Destination amount calculation
1	US dollar (USD)	250.00	Danish krone (DKK)	DKK-USD	0.21 / 0.20	USD 250.00 / 0.20 = DKK 1,250.00
2	Moldovan leu (MDL)	500.00	US dollar (USD)	MDL-USD	0.0080 / 0.0079	MDL 5000.00 x 0.0080 = USD 40.00
3	Czech koruna (CZK)	300.00	Pound sterling (GBP)	1. CZK-USD 2. GBP-USD	1. 0.050 / 0.049 2. 1.51 / 1.50	1. CZK 300.00 x 0.050 = USD 15.00 2. USD 15.00 / 1.50 = GBP 10.00
4	Swiss franc (CHF)	400.00	Euro (EUR)	CHF-EUR	0.75 / 0.74	CHF 400.00 x 0.75 = EUR 300.00
5	Euro (EUR)	200.00	Polish zloty (PLN)	PLN-EUR	0.26 / 0.25	EUR 200.00 / 0.25 = PLN 800.00
6	US dollar (USD)	80.00	Moldovan leu (MDL)	MDL-USD	0.0080 / 0.0079	USD 80.00 / 0.0080 = MDL 10,000.00
7	Danish krone (DKK)	500.00	US dollar (USD)	DKK-USD	0.21 / 0.20	DKK 500.00 x 0.20 = USD 100.00
8	Pound sterling (GBP)	400.00	Czech koruna (CZK)	1. GBP-USD 2. CZK-USD	1. 1.51 / 1.50 2. 0.050 / 0.049	1. GBP 400.00 x 1.50 = USD 600.00 2. USD 600.00 / 0.050 = CZK 12,000.00
9	Polish zloty (PLN)	350.00	Euro (EUR)	PLN-EUR	0.26 / 0.25	PLN 1,000.00 x 0.25 = EUR 250.00
10	Euro (EUR)	900.00	Swiss franc (CHF)	EUR-CHF	0.75 / 0.74	EUR 900.00 / 0.75 = CHF 1,200.00

In the above table, the first example is of a transaction where the source amount (USD 250.00) is credited to the sender. No cross-rate is involved so a USD-based rate is used. In this transaction, the source currency is USD. Therefore, as shown in the decision tree, the exchange direction is Sell. The calculation that applies is source amount (USD 250.00) / the sell rate of destination currency (0.20).

The other examples follow a similar process.

15.7 Currency Rate Delivery Service

The Visa Europe System obtains and verifies international Currency Conversion Rates from various sources around the world.

Visa Europe delivers the same Currency Conversion Rate information that it uses to Members and their Processors that subscribe to the Currency Rate Delivery Service. This optional service enables you to receive rates daily (Tuesday to Saturday) via your clearing files.

The Visa Europe System uses the Currency Conversion Rate Update Records (TC 56) to transmit updates to your conversion rate file.

Each entry contains:

- The ISO numeric currency code of the counter currency
- The ISO numeric currency code of the base currency
- The Processing Date, on which Interchange data submitted by a Member to a Visa Interchange Center (VIC) is processed for settlement by that VIC
- The buy Currency Conversion Rate and sell Currency Conversion Rate applied to the currency that day
- The currency scale factor identifier for each of the Currency Conversion Rates

For more details, see the *Dual Message System Clearing (DMSC) Technical Specifications*.

For information about how to participate in the Currency Rate Delivery Service, contact Visa Europe Customer Support.

15.8 Enhanced Interchange Data Service

The Enhanced Interchange Data Service is an optional service that enables subscribing Issuers to receive the following values in all TC x5, TC x6 and TC x7 series clearing transactions they receive from VECSS:

- **Interchange Reimbursement Fee**

To assist the reconciliation process that Issuers can perform to determine Interchange Reimbursement Fee amounts, Visa Europe provides the calculated Interchange Reimbursement Fee in each clearing transaction that Issuers receive from VECSS. Subscribing Issuers do not have to replicate fee edits or calculate Interchange fee amounts for each transaction.

- **Currency exchange rate information**

Each transaction that an Issuer receives from VECSS includes the Currency Conversion Rate that was applied to the transaction, where applicable. Participating Issuers know precisely the rate that is applied to each transaction and avoid having to reconcile each transaction to exchange rate tables in TC 56s.

For information about how to participate in this service, contact Visa Europe Customer Support.

15.8.1 Transaction types used by the Enhanced Interchange Data Service

The following key transaction types are used by the Enhanced Interchange Data Service:

TC x5, TC x6 and TC x7 - Draft Data Transactions

TCR 5 - Payment Service Data

For details, see TC 05 Draft Data Transactions in the *Dual Message System Clearing (DMSC) Technical Specifications*.

TC 04 - Reclassification Advice Transaction

TCR 9

For details, see TC 04 Reclassification Advice Transaction in the *Dual Message System Clearing (DMSC) Technical Specifications*.

15.9 Key messages and data fields

The Currency Conversion Service affects the following transaction types:

- TC x5, TC x6 and TC x7 - Draft Data Transactions, TCR 0
 - Positions 62-73 - Destination Amount
 - Positions 74-76 - Destination Currency Code
 - Positions 77-88 - Source Amount
 - Positions 89-91 - Source Currency Code
- TC x5, TC x6 and TC x7 - Draft Data Transactions, TCR 5 - Payment Service Data
 - Positions 108-115 - Source Currency to Base Currency Exchange Rate
 - Positions 116-123 - Base Currency to Destination Currency Exchange Rate

For detailed information, see the *Dual Message System Clearing (DMSC) Technical Specifications*.

16 Custom Payment Service/ATM

Custom Payment Service (CPS) is a set of transaction processing requirements that help Members to reduce fraud and exception item processing costs by ensuring the quality and integrity of the data sent in authorization and clearing messages. CPS/ATM is the specific application of the service to ATM cash disbursements.

For Acquirers, CPS/ATM protects against authorization-related chargebacks by requiring the authorization request to contain key information that fully defines the transaction conditions and helps validate Cardholder authenticity.

For Issuers, CPS/ATM increases risk control and improves account balance management. Issuers can accurately match a transaction's authorization and clearing messages using a unique Transaction Identifier that is assigned by VEAS.

All ATM cash disbursements must qualify for CPS/ATM processing. The fee applied at clearing is dependent on the transaction being compliant with the following requirements:

- For each transaction that complies with CPS/ATM requirements, the Acquirer receives a fixed Cash Disbursement Fee
- For each transaction that fails to comply with CPS/ATM requirements, the Acquirer is charged a non-compliance, or handling fee

For more information about Cash Disbursement Fees, see the applicable payment scheme or processing rules.

16.1 Related information

For further information about Custom Payment Service/ATM, see the following documents:

- *Single Message System(SMS) ATM Processing Specifications*
- *Single Message System (SMS) ATM Technical Specifications*
- *Dual Message System Authorization (DMSA) Technical Specifications*
- *Visa Europe Merchant Data Standards Manual*

16.2 Participation

CPS/ATM is available through VEAS and VECSS.

Participation is mandatory for all Acquirers, ATM Issuers and Processors.

To participate in the service, Members must meet the following requirements.

16.2.1 Requirements for ATM Acquirers

The requirements for participating in CPS/ATM depend on whether a Member is an SMS Acquirer or a dual message Acquirer:

- SMS Acquirers automatically meet the necessary technical requirements
- Dual message Acquirers must meet the requisite technical requirements for the authorization and clearing of ATM transactions, and be certified

16.2.2 Requirements for ATM Issuers

To participate in CPS/ATM, Issuers must:

- Be certified by Visa Europe, as specified in the applicable payment scheme or processing rules
- Receive and return the Transaction Identifier in the authorization response for each ATM transaction
- Be able to receive the code that identifies the ATM being used in a transaction, the details of the owner of the ATM and the ATM's location in each transaction record
- Include the Transaction Identifier for the ATM transaction in all chargebacks

16.2.3 Testing and certification

CPS/ATM certification is available for dual message Visa and Visa/Plus ATM Acquirers and Issuers.

For more information, Members should contact Visa Europe Customer Support.

16.2.4 Service monitoring

Although Members should review their own processing as it relates to participation in CPS/ATM, Visa Europe also reviews ATM activity.

For more information, Members should contact Visa Europe Customer Support.

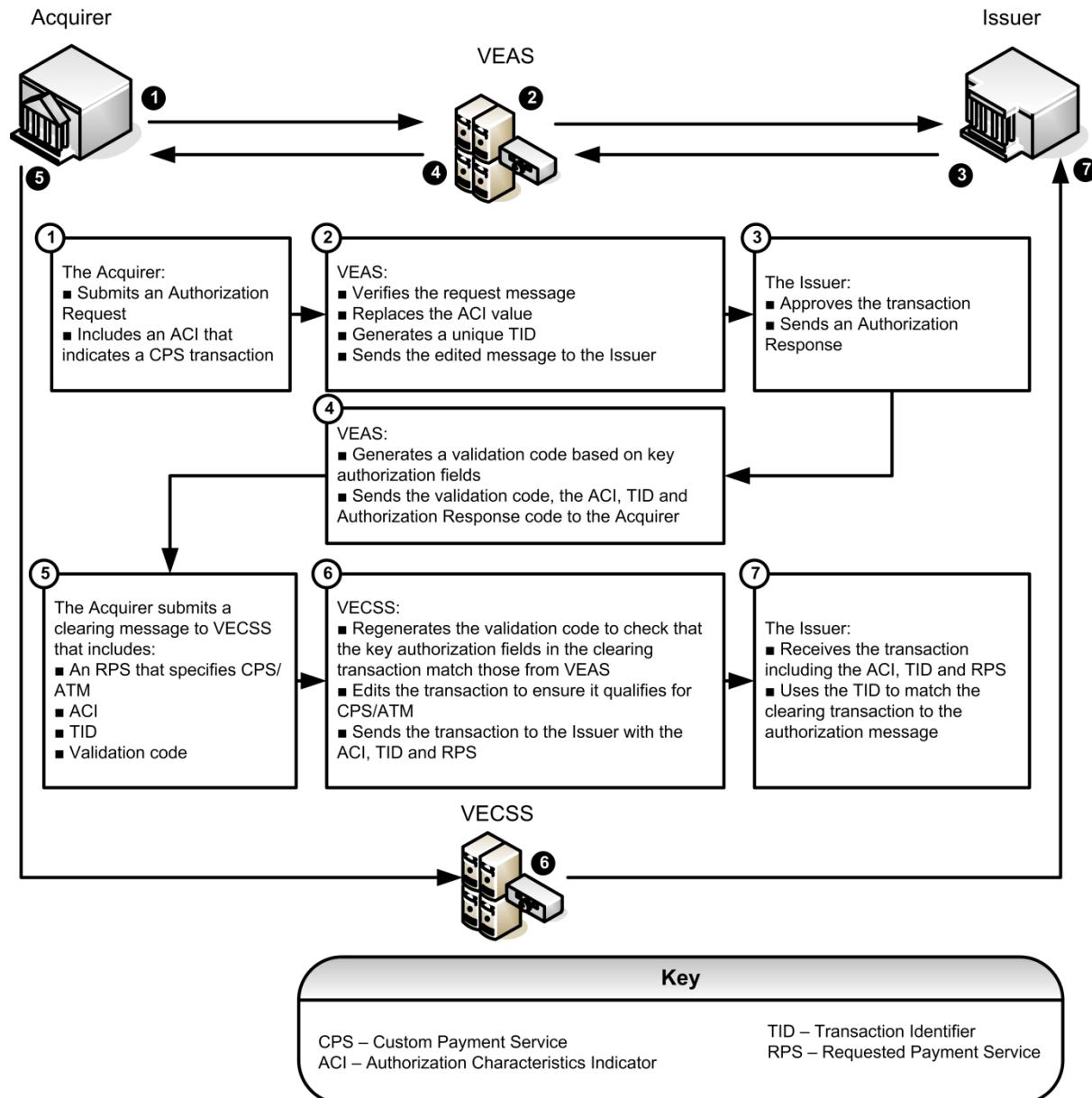
16.2.5 Planning and implementation

For more information, Members should contact Visa Europe Customer Support.

16.3 How the service works

The following diagram provides a summary of how the CPS/ATM works for dual message transactions, where the Acquirer and Issuer are certified CPS/ATM participants.

Figure 30: Overview of how CPS/ATM works



1. Acquirer sends an authorization request for a cash disbursement with an authorization characteristics indicator (ACI) of Y (transaction requests participation) to VEAS.
2. VEAS edits the message (see [CPS/ATM qualification requirements for authorization](#) on page 136), and forwards it to the Issuer.
 - If the message meets CPS/ATM requirements, VEAS changes the ACI to E (qualified), and generates a unique Transaction Identifier (TID)
 - If the message does not meet CPS/ATM requirements, VEAS changes the ACI to N (not qualified), and generates a unique Transaction Identifier (TID)

3. The Issuer verifies the request, and sends a response message to VEAS including an authorization response code.
 - The Issuer can approve or decline non-qualifying requests
4. VEAS generates a validation code based on key authorization fields, and forwards the authorization response including the validation code with the ACI, TID and authorization response code to the Acquirer. If the message is not qualified, VEAS substitutes a downgrade reason code (DRC) for the validation code, and forwards it to the Acquirer.

Note The validation code is not present in advice messages sent to Issuers.

5. The Acquirer submits a clearing message to VECSS including a requested payment service (RPS) code of 9 (CPS/ATM).

The clearing message includes the ACI, the TID and the validation code received in the authorization response.

6. To verify that the key authorization fields contained in the clearing transaction match those sent in the authorization request, and in the CPS fields received in the outgoing response message, VECSS regenerates the validation code. VECSS uses the key field values from the clearing transaction submitted by the Acquirer and matches the result against the Acquirer-provided validation code. It also applies edits to check that the transaction qualifies for CPS/ATM (see *CPS/ATM qualification requirements for clearing* on the next page).

If a transaction meets requirements, the Cash Disbursement Fee is applied.

If a transaction fails to meet requirements, it is reclassified as non-compliant or returned to the Acquirer for correction and re-submission:

- If a transaction is reclassified, the Acquirer must pay a non-compliance or handling fee
- If a transaction is returned to the Acquirer, resubmitted as a compliant transaction and cleared within three calendar days, the Acquirer receives the Cash Disbursement Fee

- A qualified transaction submitted after three calendar days will not be returned to the Acquirer but will be settled and assessed a handling fee

Check	Result
Validation code check	Failed validation code check and not cleared within two days - transaction is reclassified Failed validation code check and has cleared within two days - transaction is returned to Acquirer for correction and resubmission
Amount tolerance check The amount submitted in the clearing message must be equal to or less than the amount authorized	Failed amount tolerance check and not cleared within two days - transaction is reclassified Failed amount tolerance check and has cleared within two days - transaction is returned to Acquirer for correction and resubmission.
General timeliness	Must be cleared within three calendar days

The transaction, including the ACI, the TID and the RPS, is sent to the Issuer.

Note The transaction component record (TCR) 5 is included as part of the draft data. This record includes the TID.

7. The Issuer uses the TID to match the clearing transaction with the authorization request.

16.3.1 CPS/ATM qualification requirements for authorization

To qualify, an authorization request must comply with the following requirements.

Table 17: CPS/ATM qualification requirements for authorization

Description	Requirement
Track 2 magnetic stripe or chip card track data	Must be included in the request message. If field 35 - Track 2 Data is not present, the message is rejected with reject code 0291 (field missing)
Merchant Category Code (MCC)	6011 (ATM)
ATM location and card acceptor data	Must be present in fields 41 - Card Acceptor Terminal Identification, 42 - Card Acceptor Identification Code and 43 - Card Acceptor Name/Location
Authorization characteristics indicator (ACI)	Must have a value of Y

16.3.2 CPS/ATM qualification requirements for clearing

To qualify, the clearing message must comply with the following requirements.

Table 18: CPS/ATM qualification requirements for clearing

Description	Requirement
Authorization characteristics indicator (ACI)	E
Requested Payment Service (RPS)	9
Transaction Identifier (TID) from the authorization message	Must be present
Validation code in authorization message and clearing record	Must match
Reimbursement attribute	G (Visa/Plus), or H (Visa)
Number of authorizations per clearing transaction	One authorization per clearing transaction
Clearing timeliness	Three calendar days or less
Amount tolerance factor	Must be met. The amount submitted in the clearing message must be equal to or less than the amount authorized

16.3.3 Further Clearing checks

The following are the initial checks done at the edits level for CPS/ATM transactions. If these edits are not met, the transaction will be returned with the appropriate reason code. These are applicable for ATM original transactions and reversals (Usage Code = 1), and edits, where MCC = 6011, RPS = 9, and ACI = E.

Table 19: Edit level checks for CPS/ATM transactions

Edit	Action to follow, failing the edit
TCR 5 should be present for all domestic transactions within the Europe region	Return to Acquirer
Authorization date must be valid	Return to Acquirer
Purchase date must be valid	Return to Acquirer
Authorization currency code must equal source currency code	Return to Acquirer
Purchase date must not be later than authorization date by more than one day	Return to Acquirer
Authorized amount must be valid	Return to Acquirer

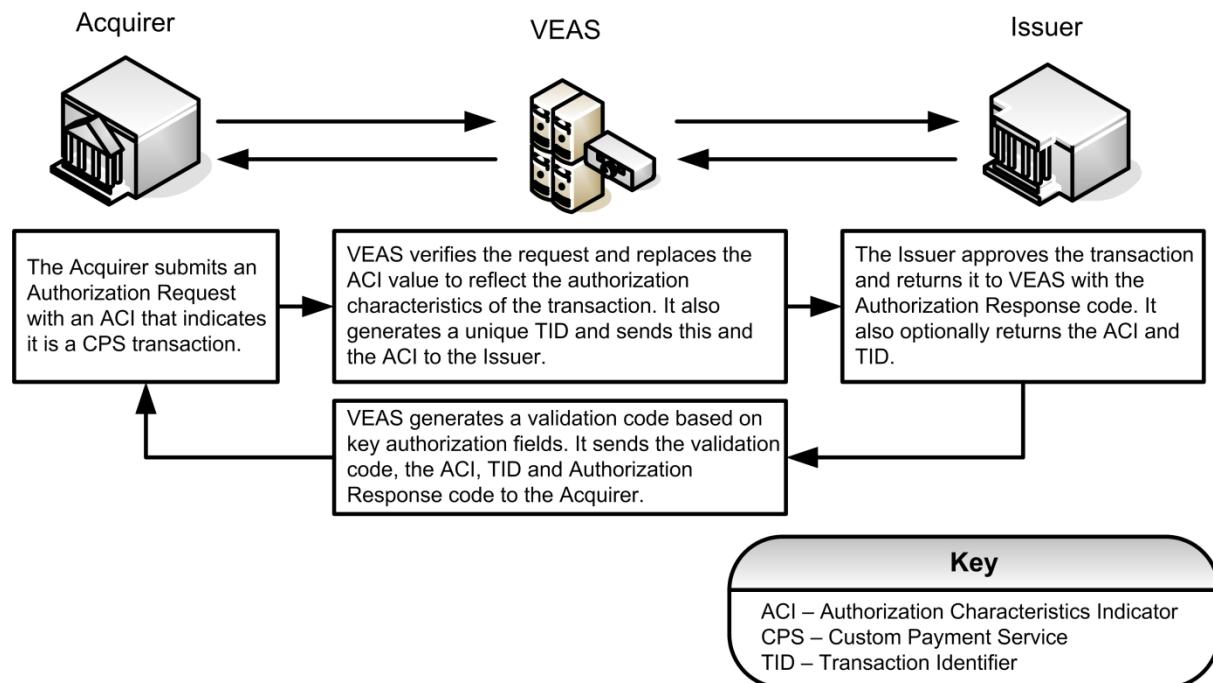
16.4 Process flows

This section illustrates a transaction from authorization through clearing in a dual message environment.

16.4.1 Process flow for CPS/ATM authorization

The following diagram illustrates the CPS/ATM process flow for authorization in a dual message environment.

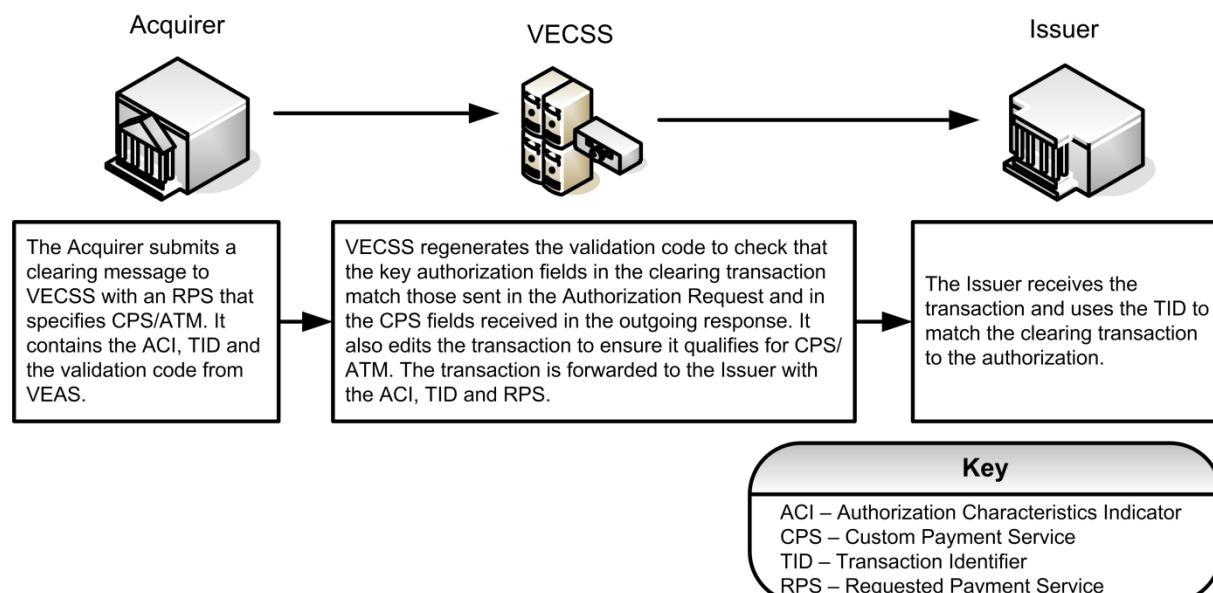
Figure 31: Process flow for CPS/ATM authorization



16.4.2 Process flow for CPS/ATM clearing

The CPS/ATM process flow for clearing in a dual message environment is shown in the following diagram.

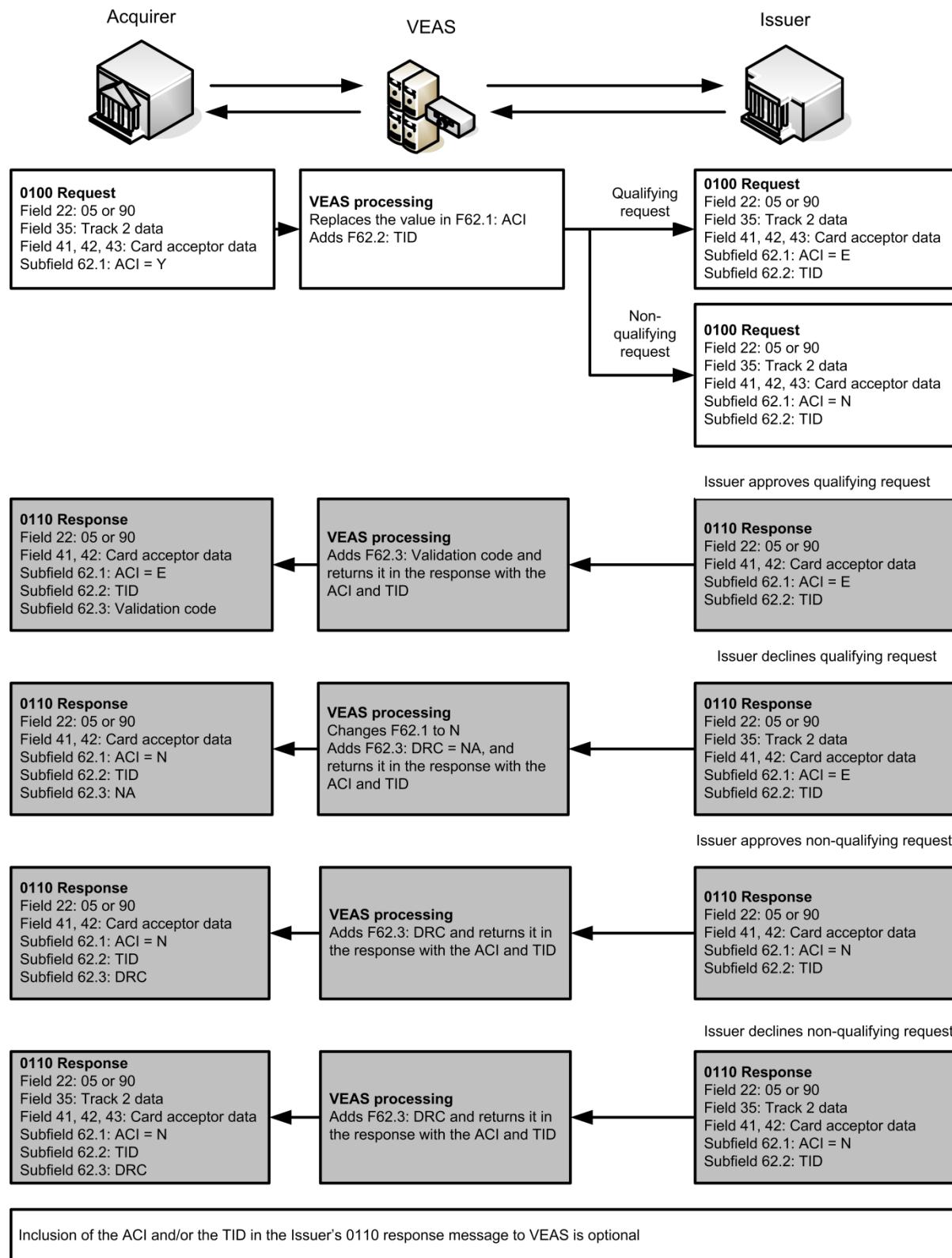
Figure 32: Process flow for CPS/ATM clearing



16.5 Message flows

The following diagram gives a simplified view of the CPS/ATM message flow for authorization in a dual message environment.

Figure 33: Message flow for CPS/ATM authorization in a DMSA environment



16.6 Key data fields

The following key data fields are used by the Custom Payment Service/ATM. For detailed information, see the Visa Europe technical specifications.

Data field 62 - Custom Payment Service Fields

- **Subfield 62.1 - Authorization Characteristics Indicator (ACI)**

This data field is used by the Acquirer to indicate a CPS/ATM transaction. VEAS changes the code to reflect the results of the CPS evaluation.

- **Subfield 62.2 - Transaction Identifier**

The transaction identifier (TID) is a unique system-generated identifier assigned to each transaction that links original authorizations to subsequent messages such as reversals. TIDs are based on the date and time.

- **Subfield 62.3 - Validation Code**

The system-generated validation code is added only to DMSA 0110 authorization responses and ensures that the values in the authorization requests key CPS fields match their respective fields in the DMSC deferred clearing message.

If an authorization request fails CPS qualification but is nevertheless approved by the Issuer, DMSA inserts the CPS downgrade reason code (DRC) instead of the validation code in the response message to the Acquirer. The DRC is not passed to DMSC in the deferred clearing message; the Acquirer enters spaces instead.

16.6.1 Key field cross reference

The following table shows how the Dual Message System Authorization fields are carried forward by the Acquirer to populate the related fields in the Dual Message System Clearing records. The table also shows which key CPS/ATM fields are used to generate the validation code.

Table 20: Custom Payment Service/ATM - key field cross reference

Dual Message System Authorization (DMSA) message fields		Dual Message System Clearing (DMSC) transaction fields		Used to determine validation code
DMSA field	Field name	DMSC field	Field name	
2	Primary Account Number	TCR 0, positions 5-20	Account Number	✓
3	Processing Code (Transaction Type, positions 1-2) A value of 01 (with a value of 6011 in field 18 - Merchant Type) indicates that an ATM Transaction code is to be used in the DMSC field.	TCR 0, positions 1-2	Transaction Code	
3	Processing Code (Account Type 'from,' positions 3-4) The first digit of the DMSA value must be used in the DMSC field.	TCR 1, position 130	ATM Account Selection	✓
4	Amount, Transaction In the case of a misdispense, field 61.1 contains the amount of the actual cash dispensed, and field 4 contains the amount of the original authorization. Field 4, the Authorized Amount, must be provided in the DMSC TCR 5 record.	TCR 5, positions 20-31	Authorized Amount	✓
18	Merchant Type	TCR 0, positions 133-136	Merchant Category Code	
22	POS Entry Mode Code (position 1-2)	TCR 0, positions 162-163	POS Entry Mode	
28	Amount, Transaction Fee	TCR 4, positions 51-58	Surcharge Fee	✓
32	Acquiring Institution Identification Code	TCR 0, positions 28-33	Acquirer BIN (in the Acquirer Reference Number)	✓
35	Track 2 Data Track 2 is required or VEAS rejects the message.	Not applicable	Not applicable	

Table 20: Custom Payment Service/ATM - key field cross reference (continued)

Dual Message System Authorization (DMSA) message fields		Dual Message System Clearing (DMSC) transaction fields		Used to determine validation code
DMSA field	Field name	DMSC field	Field name	
38	Authorization Identification Response	TCR 0, positions 152-157	Authorization Code	
39	Response Code	TCR 5, positions 35-36	Authorization Response Code	
41	Card Acceptor Terminal Identification	TCR 1, positions 96-103	Terminal ID	
42	Card Acceptor Identification Code (Contains ATM owner's name)	TCR 1, positions 81-95	Card Acceptor ID	
43	Card Acceptor Name/Location: ATM Location (positions 1-25) City Name (positions 26-38) Country Code (positions 39-40)	TCR 0, positions 92-116 TCR 0, positions 117-129 TCR 0, positions 130-132	Merchant Name Merchant City Merchant Country Code	
49	Currency Code, Transaction	TCR 5, positions 32-34	Authorization Currency Code	✓
54	Additional Amounts	Not applicable	Not applicable	
59	National POS Geographic Data (positions 1-2) (US region only)	TCR 0, positions 142-144	Merchant State / Province Code (US region only)	
62.1	Authorization Characteristics Indicator (ACI)	TCR 0, position 151	Authorization Characteristics Indicator (ACI)	✓
62.2	Transaction Identifier	TCR 5, positions 5-19	Transaction Identifier	✓

Table 20: Custom Payment Service/ATM - key field cross reference (continued)

Dual Message System Authorization (DMSA) message fields		Dual Message System Clearing (DMSC) transaction fields		Used to determine validation code
DMSA field	Field name	DMSC field	Field name	
62.3	Validation Code	TCR 5, positions 37-40	Validation Code	
	Not applicable	TCR 0, position 168	Reimbursement Attribute	

17 Euro Area Net Settlement Service

The Euro Area Net Settlement Service (EANSS) is part of the Visa Europe Settlement Service (VSS) which performs settlement for transactions that are cleared through Dual Message System Clearing (DMSC) and the Single Message System (SMS) in a single, centralised service.

Members that participate in the EANSS benefit from Processing Date or same day settlement for qualifying euro transactions. This is earlier than settlement through the International Settlement Service, which takes place two days after the Processing Date.

17.1 Related information

For further information about the Visa Europe Settlement Service, of which the EANSS is a part, see the following documents:

- *Visa Europe Settlement Service (VSS) User's Guide*
- *Visa Europe Settlement Funds Transfer Guide*

To arrange to implement this service, contact Visa Europe Customer Support.

17.2 Participation

The EANSS is available through VECSS.

Participation is:

- Mandatory for Members and their Processors in the Economic and Monetary Union (EMU) countries whose transactions meet the following criteria:
 - Clear through the Visa Europe Clearing and Settlement Service (VECSS)
 - Have a Transaction Currency and a Settlement Currency of euros
 - Issuer, Acquirer and point-of-transaction are within the Europe region
- Optional for Members and their Processors that are not located within an EMU country

17.3 How the service works

Note Before settling with Visa Europe you must complete the Settlement Funds Transfer forms.

The main steps in the EANSS are:

1. The Visa Europe System collects Interchange Files containing transactions from Members.
2. DMSC and SMS perform clearing and editing on all transactions.
3. After the close of the Settlement Window, VECSS sends the cleared transactions to VSS.

4. VSS processes the settlement records and delivers VSS settlement reports that detail the net Settlement Amount to Members' Visa Extended Access Servers (EA Server) on a daily basis.

Note You can use your VSS reports or log into Visa Online to view your settlement position on the Daily Net Settlement Service Positions (DNSSP) page.

5. Funds transfer takes place. During this step, funds are paid from Members in a net debit (issuing) position, and paid to Members in a net credit (acquiring) position.

17.3.1 Clearing and settlement timing

See the *Visa Europe Settlement Service (VSS) User's Guide* for details about the settlement processing schedule for the EANSS, including its cut-off time, file delivery time and Settlement Date.

Important If you participate in the EANSS, review your EA Server collection times to ensure your outgoing EANSS Interchange Transaction Files (ITF) can be collected before the close of the Settlement Window for the euro area net.

The EANSS conforms to the European Central Bank (ECB) TARGET (Trans-European Automated Real-time Gross Settlement Express Transfer System) holiday schedule.

17.3.2 Funds transfer

Funds transfer is the movement of funds between a Member's Settlement Bank and Visa Europe's Settlement Bank for the purpose of settlement. The funds transferred represent the net position of a Member's credits and debits:

- Members in a net debit (issuing) position pay funds
- Members in a net credit (acquiring) position receive funds

For qualifying euro transactions the EANSS performs Processing Date 'Day 0' (same day) settlement. Funds are moved on working days.

An FTSRE can only have funds transferred to or from a single settlement account. However, if a Member has several FTSREs that belong to different settlement services, each FTSRE can use the same account or use different accounts.

Within the euro area net, funds are settled in euros with a Member-selected Settlement Bank.

Note The Member must be the account owner of the selected bank and it must be linked to the SWIFT network.

17.3.2.1 Paying funds to Visa Europe

Members are responsible for paying all net debit (issuing) positions on the EANSS.

These positions are settled as follows:

1. You determine your settlement position from your VSS reports or from the DNNSP page on Visa Online.
2. You create a funds transfer from your Settlement Bank to the Settlement Bank of Visa Europe.

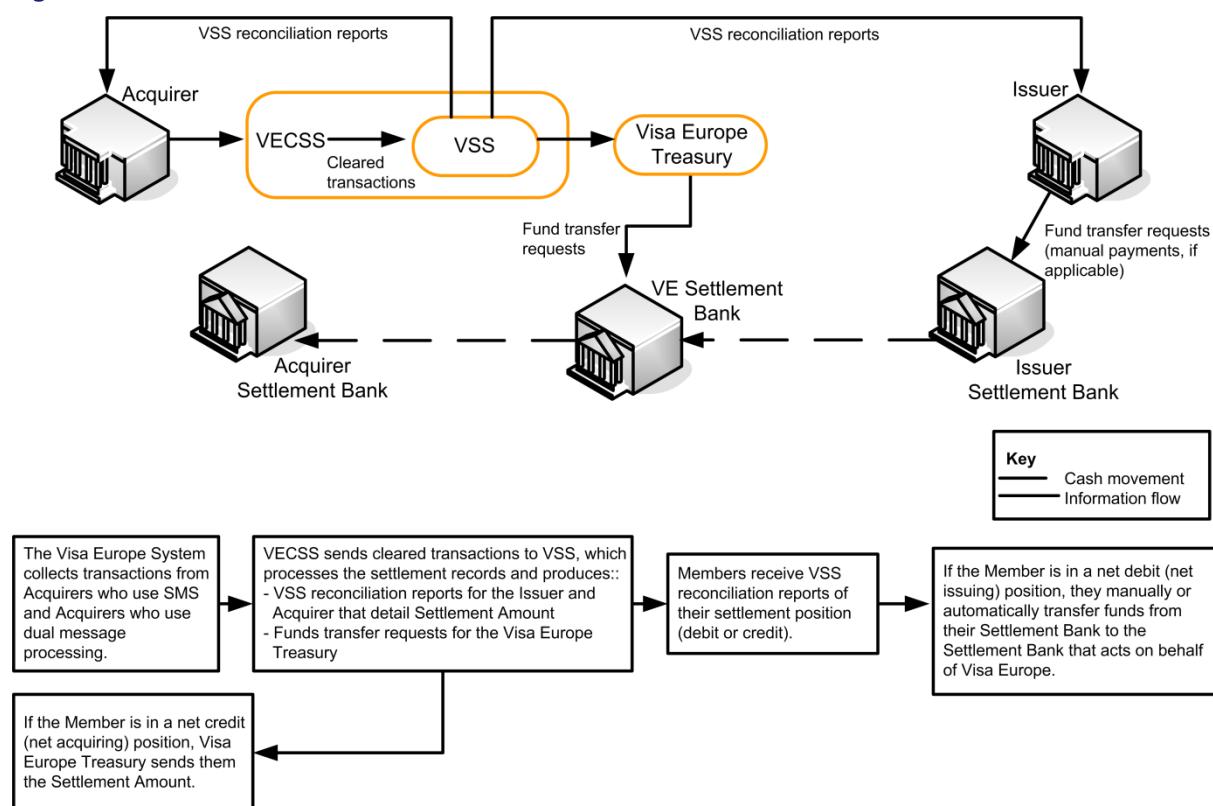
17.3.2.2 Receiving funds from Visa Europe

Visa Europe's Treasury forwards the amount owed to Members that are in a credit position.

17.4 Process flows

The following diagram illustrates the process flow for the EANSS.

Figure 34: Process flow for the Euro Area Net Settlement Service



18 File Collection and Delivery Service

The main steps in the File Collection and Delivery Service are:

1. **Collection:** Visa Europe collects outgoing Interchange Files from Members or their Processors. Files are either collected at pre-arranged times or can be based on manual collection initiated by Visa Europe Operations.
2. **Delivery:** After clearing and settlement, Visa Europe automatically delivers the Interchange Files according to the delivery options chosen by the Member that receives the files.

18.1 Related information

For further information about the File Collection and Delivery Service, see the following documents:

- *Introducing the Visa Europe Clearing and Settlement Service*
- *Dual Message System Clearing (DMSC) Technical Specifications*
- *Dual Message System Clearing (DMSC) Reports*
- *Introducing DMSA and SMS Transactions*

18.2 Participation

The File Collection and Delivery Service is available through VECSS to users of DMSC.

Participation is:

- Mandatory for Members or their Processors using DMSC to process International Transactions
- Optional for Members or their Processors using DMSC to process Visa Europe Transactions, including Domestic Transactions
- Not applicable to Members using SMS

To participate in the service, Members must meet the following requirements.

18.2.1 Planning and implementation

Before proceeding, you must:

- Contact Visa Europe Customer Support to arrange for your BINs to be configured in VECSS
- Arrange with Visa Europe the times when you want the Visa Europe System to poll your Visa Extended Access Server (EA Server) to collect your outgoing Interchange Files
- Install the Visa-specific application, Edit Package

18.2.2 Testing and certification

Files must be run through the Edit Package in test mode.

18.2.3 Service monitoring

File collections and deliveries are monitored by the Visa Interchange Center (VIC).

18.3 How the service works

The File Collection and Delivery Service enables you to:

- Choose how and when Interchange Files are collected and delivered
- Package separately data that is critical to your processing
- Route specific transactions to different locations for faster processing

Note In addition to the above file collection and delivery options, you can also contact Visa Europe Customer Support to manually redeliver an existing file or to manually collect a file. Any other delivery options that you have established for that file remain in effect.

18.3.1 File collection

Throughout the day, Visa Europe collects and receives Interchange Files that contain transactions from Members.

VECSS connects to your EA Server and collects the outgoing Interchange Files at pre-established times. These times are configured in the VECSS Member Configuration tables.

To increase efficiency, you can divide the outgoing Interchange File into multiple files that are collected at different times.

18.3.2 File delivery

For each settlement service in which you participate, you automatically receive delivery files at the end of the Settlement Cycle. For example, if you participate in National Net Settlement (NNSS), you receive all data settled by that NNS after the close of its Settlement Window. This may be earlier than the default International Settlement Service (ISS) window. For example Swedish NNS files are sent after 08:00 GMT (7:00 GMT in summer), whereas ISS files are sent after 11:00 GMT (10:00 GMT in summer).

Normally, transaction data and settlement reports are delivered simultaneously. However, you can also choose from a number of options to suit your needs, such as having specific types of data delivered in advance of settlement.

Examples of situations where this might be required include:

- To balance the workload
- To easily identify customised files containing only items that were returned by VECSS
- Where particular transactions, such as Currency Conversion Rate Update Records (TC 56), are critical to your processing

The following table lists the options for file delivery.

Table 21: Options for file delivery

Option	Description
Standard file delivery	The complete set of delivery files, that is, all your transaction data and settlement reports are delivered in a single file.
Delivery by volume	Data is delivered based on the volume processed
<i>Customised file delivery</i> below	Enables you to customise your delivery files based on a list of file types pre-defined by Visa Europe. The file types that you request are delivered as separate files. If required, you can have some of these files delivered as soon as they are available, in advance of the relevant Settlement Window.
<i>Split routing</i> on page 151	Enables you to deliver specific file types pre-defined by Visa Europe to multiple Processing Centres

You can choose any combination of the above options.

18.3.2.1 Standard file delivery

Standard file delivery is the default delivery option that you receive if you do not ask for any customisation. It is also known as undifferentiated (UNDIF file type) delivery. For each settlement service in which you participate, you receive a single file that contains all data, after the close of the relevant Settlement Window. If you need to receive any of the data in a separate file, you must request customised delivery.

18.3.2.2 Delivery by volume

Delivery by volume enables you to set a maximum file size for your incoming Interchange Files per settlement service in which you participate. For example, if you have requested a maximum file size of 100,000 transactions but Visa Europe has 101,000 transactions to deliver to you on a particular day, and for a particular settlement service, Visa Europe will send you two files. The first will contain 100,000 transactions and the second will contain only 1,000 transactions. Both files are sent at the same time, after the relevant Settlement Window closes.

18.3.2.3 Customised file delivery

This option enables you to customise delivery files based on a list of pre-defined file types. This means that transactions of the same file type are delivered in a single file that is separate from the standard delivery file. For example, if you request currency rates as a customised delivery file, instead of being delivered as part of the standard delivery file, they are delivered in a separate file. All the rest of your data is delivered in a standard delivery file.

Customised file delivery also provides the option of expedited delivery. This option provides immediate delivery of selected customised delivery files, regardless of the normal delivery schedule. It enables you to receive selected files as soon as they are ready to be delivered.

You can choose the following types of customised delivery files.

Table 22: Customised delivery file types

File type	Code	Expedite option available	Business description
DMSA advice messages	BI	No	Bulk file delivery of authorization advice messages produced by stand-in processing (STIP)
DMSA TC 33 report	BA	Yes	A report of the Visa Europe System generated multi-purpose messages (TC33s)
CDC	CD	Yes	Data capture advice messages (TC 57s), used by Visa Europe to send to an Acquirer data received from a third-party Data Capture Service about a transaction, so the Acquirer can submit the transaction as a sales draft or representment (TC 05).
Currency rates	CU	Yes	Daily (Tuesday to Saturday) Currency Conversion Rates that are applied to transactions in VECSS (TC 56s)
Debit reports	DR	Yes	SMS detail reports
Edit Package updates	EP	No	Updates to Edit Package. For more information, see the Edit Package documentation.
Settlement reports (Print)	LR	No	Print-ready settlement reports
Settlement reports (Machine)	MR	No	Machine-readable settlement reports
National Net settled	NN	No	Transaction data used in National Net Settlement
National Settlement reports	NS	Yes	National Net Settlement reports
RDMS	RD	No	Member reports from the Report Distribution Management System
Debit raw data	RW	Yes	Detailed, machine-readable SMS transaction data

Table 22: Customised delivery file types (continued)

File type	Code	Expedite option available	Business description
Settlement reports	SR	No	Combined print-ready and machine-readable settlement reports
UK electronic HCF	UN	Yes	UK electronic hot card file (a file containing a list of UK card/account numbers that have an associated pickup code)

For more information about the file types, see the *Introducing SMS and DMSA Transactions* manual.

18.3.2.4 Split routing

With split routing, you can deliver specific Interchange File types to different Processing Endpoints.

Split routing codes are set up at the BIN level. To use split routing, you can use one or more of the following codes for each BIN.

Table 23: Split routing codes

File type	Code
ATM Back-Office	AB
ATM Originated	AO
Back-Office	BK
VDAS Route List Acquirer	CA
VDAS Route List issuer	CI
RFC Acquirer	RA
RFC Issuer	RI
Split Collection	SC
ATM Format Conversion: Other	AF
ATM Format Conversion: Credit	FC
ATM Format Conversion: Debit	FD

18.4 Process flows

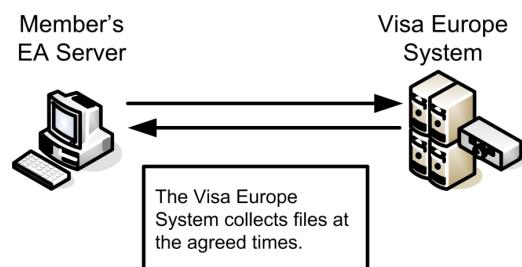
The File Collection and Delivery Service involves the following process flows:

- [Process flows for collection](#) on the next page
- [Process flows for delivery](#) on the next page

18.4.1 Process flows for collection

The Visa Europe System polls a Member's EA Server to collect the outgoing Interchange Files at the times that were agreed with Visa Europe and set up in the VECSS Member Configuration tables. The following diagram illustrates standard collection.

Figure 35: Process flow for standard collection



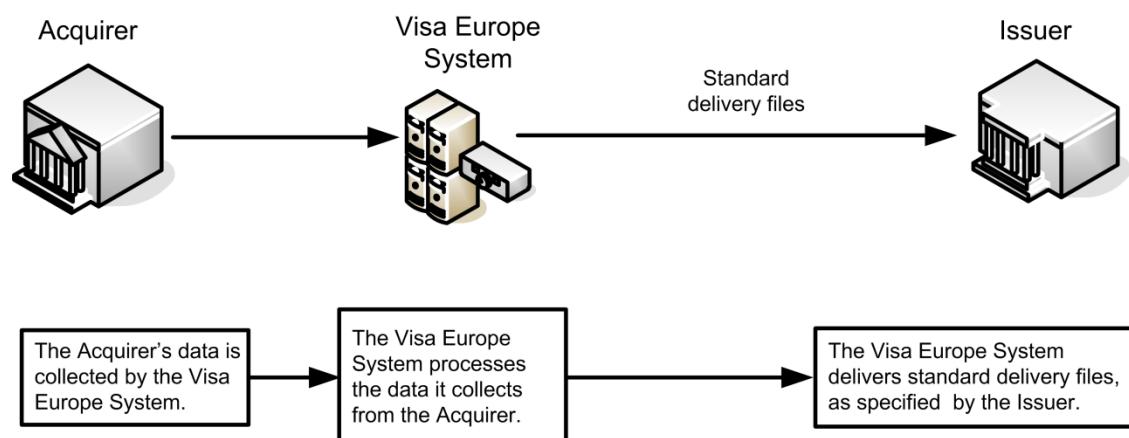
18.4.2 Process flows for delivery

The main file delivery options that can be chosen by Members that use the File Collection and Delivery Service are illustrated in the following sections.

18.4.2.1 Process flow for standard delivery

The following diagram illustrates the standard file delivery process from Acquirer to Issuer.

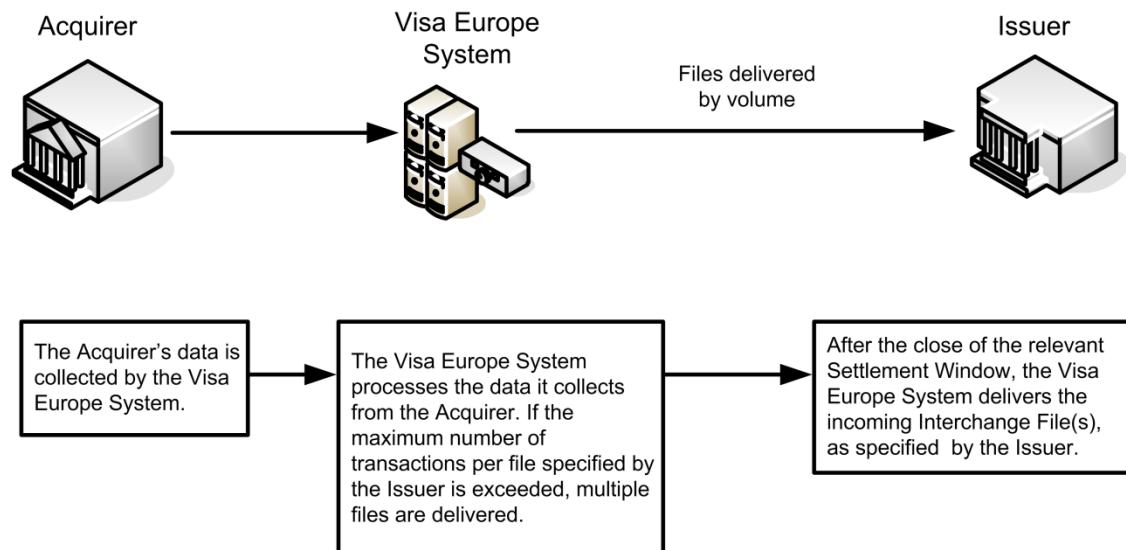
Figure 36: Process flow for standard delivery



18.4.2.2 Process flow for delivery by volume

The following diagram illustrates the process for delivery by volume from Acquirer to Issuer.

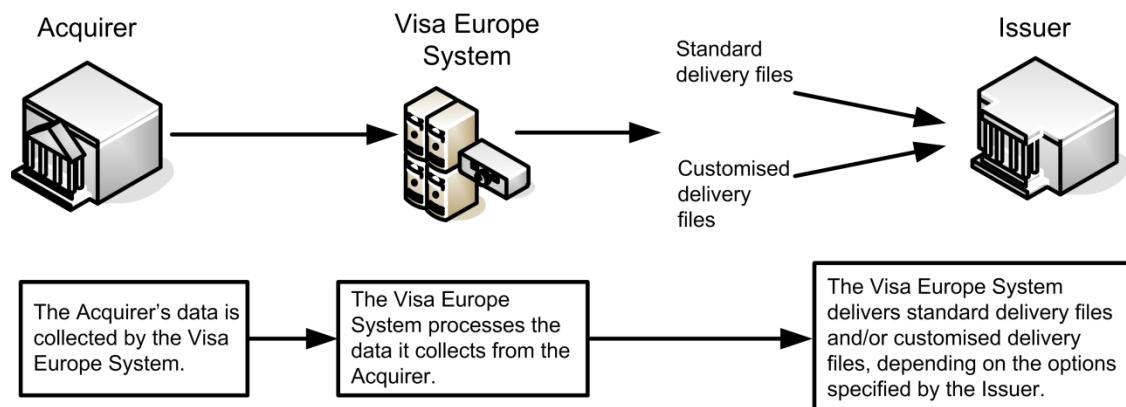
Figure 37: Process flow for delivery by volume



18.4.2.3 Process flow for customised delivery

The following diagram illustrates the customised file delivery process from Acquirer to Issuer.

Figure 38: Process flow for customised delivery



18.4.2.4 Process flow for split routing

Visa Europe assigns a priority to split routing codes to establish priority ranking. Where two split routing options have overlapping selection criteria, the routing option with the higher priority, indicated by a higher selection sequence number, is used to route the transactions that qualify for both options.

Split routing codes are set up at the BIN level.

Example

The ATM Originated (AO) file type selects all transactions that originate at an ATM (both Issuer and Acquirer, original and back-office) and it has a selection sequence number of 30.

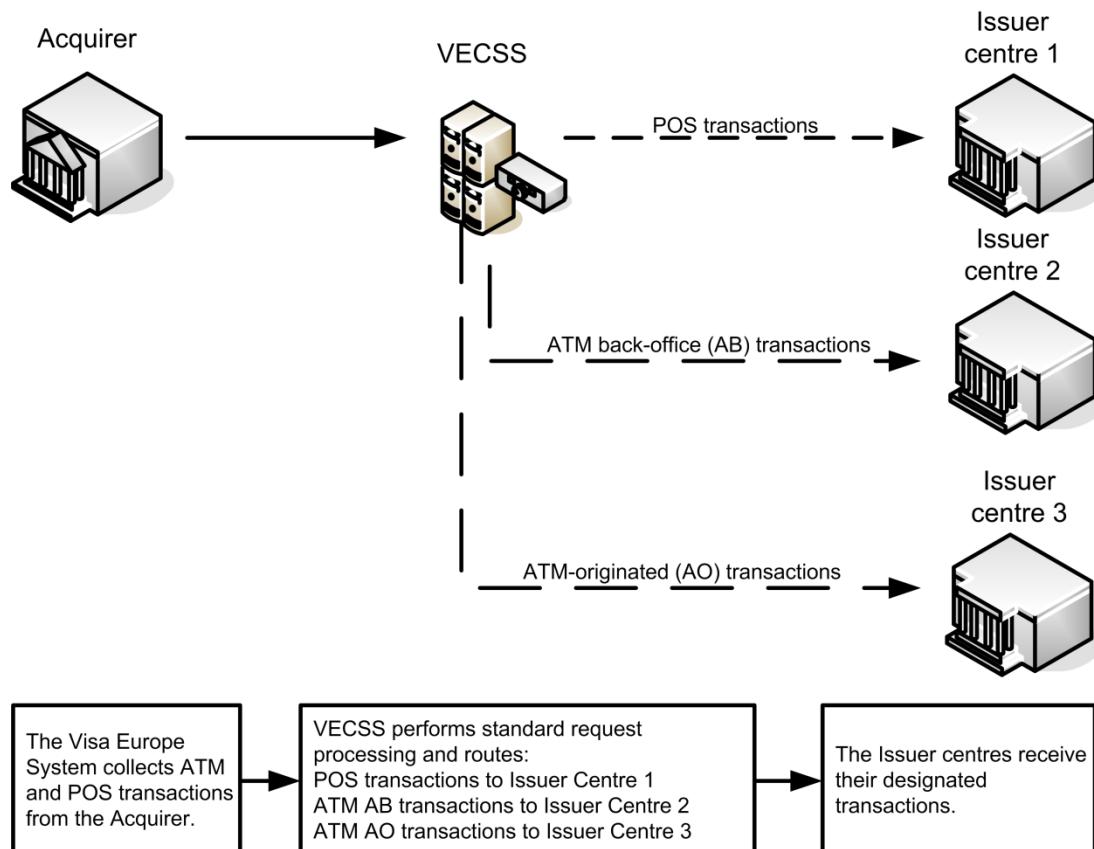
The ATM Back-Office (AB) split routing code selects only back-office transactions that originate at an ATM, but it has a higher selection sequence number of 34.

If issuer BIN $4nnnn1$ has been set with AO routing to BIN $4nnnn3$ and AB routing to BIN $4nnnn2$, (where n represents a single digit), then:

- The BIN $4nnnn1$ receives all POS transactions
- The AB BIN $4nnnn2$ receives all ATM back-office transactions
- The AO BIN $4nnnn3$ receives only ATM original transactions

The following diagram illustrates this example.

Figure 39: Example of split routing



19 Fraud Reporting System

Fraud occurs when an individual who is not the Cardholder or designee uses a card or its account number to obtain goods or services without the Cardholder's consent. Fraud also occurs when a card is obtained through misrepresentation of identification or financial status.

The Fraud Reporting System (FRS) provides Members and their Processors with a convenient, electronic way to report, track and analyse fraudulent transactions. It consolidates fraud information to help Members detect fraud patterns and reduce losses. It also enables Visa Europe to monitor fraud and develop new countermeasure programmes. FRS is mandatory for all Members.

You can report fraudulent transactions to FRS using:

- Dual Message System Clearing (DMSC)
- Single Message System (SMS)
- Visa Resolve Online (VROL)

Fraud reports can be submitted, reviewed and corrected using VROL. For more information, see the VROL documentation.

Note The system used to report fraud is independent of the system used for the original transaction. For example, you can send a TC 40 transaction to report a fraudulent 0200 full financial message that was submitted via SMS.

Members ensure eligibility for maximum chargeback rights, as described in the applicable payment scheme or processing rules, by correctly reporting fraudulent transactions. To maximise protection from fraudulent losses, it is important that you report fraud accurately, quickly and comprehensively.

19.1 Related information

For further information about FRS, see the following documents:

- *Fraud Reporting System (FRS) User's Guide*
- *Visa Resolve Online Member Implementation Guide*
- *Visa Resolve Online User's Guide*

19.2 Participation

Participation in FRS is mandatory for Issuers, Acquirers and Processors. To participate in FRS, Members must meet the following testing, compliance and implementation requirements.

19.2.1 Testing and certification

All new Issuers must complete FRS certification. This includes adding, changing and deleting an account number to or from FRS, receiving reports, and correcting any rejects and warnings from FRS.

The Visa Member Testing Service (VMTS) provides testing and certification assistance for FRS participants. To make arrangements for testing, contact Visa Europe Customer Support.

19.2.2 Service compliance

Service compliance requirements apply to FRS. For detailed information, see Fraud Activity Reporting in the applicable payment scheme or processing rules.

Note At Visa Europe's discretion, Members that fail to comply with the requirements set out in the applicable payment scheme or processing rules may lose their chargeback rights and be subject to fines and penalties.

19.2.3 Planning and implementation

To use the FRS, participants must be:

- Connected to the Visa Europe System
- Able to create TC 40 (DMSC) transactions or 9620 (SMS) Fraud Advice messages

Issuers and Acquirers must comply with the fraud reporting rules as defined in the applicable payment scheme or processing rules.

Important You must report all confirmed fraud activity with all original transaction data.
Do not modify or omit available original transaction information.

19.3 How the service works

Members must report all confirmed fraudulent transactions to Visa Europe.

To report fraud, you must complete the following steps:

1. Gather the required clearing data for the transaction(s) you want to report as fraud.
2. Before you submit a new transaction, check your records to make sure your organisation has not already reported it. If you try to add an existing transaction as a new one, FRS will reject the transaction with reject status code R80.
3. Submit the completed fraud advice message to Visa Europe using one of the following methods:
 - Single Message System (SMS)
 - Dual Message System Clearing (DMSC)
 - Visa Resolve Online (VROL)

FRS applies correctly submitted fraud transactions to the Visa Fraud Master File. Transactions that require additional verification or correction are accepted, but are flagged as warnings. It rejects any that contain serious errors and notifies the relevant Member in daily or weekly Fraud Activity reports.

4. Review fraud reporting in the daily or weekly Fraud Activity reports to determine whether the reported transaction was:
 - Accepted
 - Flagged as a warning (accepted but may require additional verification or correction and resubmission)
 - Rejected and requires correction and resubmission
5. Correct and resubmit any transactions that are reported as containing errors.

19.3.1 Reporting fraud correctly

When reporting fraud, you are required to report specific information about transactions, such as Transaction Amount and Transaction Date. Required information is obtained from several sources, including the Cardholder, the original transaction draft and the authorization message.

To report fraud correctly, you must also follow some basic rules including those described here. For more detailed information about reporting fraud, see the *Fraud Reporting System (FRS) User's Guide*.

19.3.1.1 Assign the correct notification codes

Use the correct Notification Code (NC) in the fraud advice message to determine whether the transaction is:

- Added (NC 1 and NC 2)
- Changed (NC 3)
- Deleted (NC 4)
- Reactivated (NC 5)

19.3.1.2 Assign account sequence numbers consecutively

Fraud transaction account sequence numbers can be assigned by Visa Europe or by Members. A maximum of 1000 transactions can be reported on a given account.

If you assign account sequence numbers, you must assign transactions **in consecutive order as you receive them**, beginning with 001.

19.3.1.3 Do not change the Merchant Name field

Do not modify the Merchant Name field with special codes or symbols.

19.3.1.4 Keep to the reporting timeframe

Each day, FRS adds the reported transactions to the Visa Fraud Master File and assigns a posting date on the day they are processed. The posting date is used to determine how many days from the Transaction Date the transaction is being reported and whether the fraud transaction meets the reporting timeframes.

Issuers must report all confirmed fraudulent transactions as soon as possible, but no later than 60 days after the Transaction Date.

For further details about the mandatory fraud reporting timeframes, see Fraud Activity Reporting in the applicable payment scheme or processing rules.

The way FRS handles transactions depends on when they are reported.

FRS status of reported transactions

The following table shows the FRS status of transactions reported at different times.

Table 24: FRS status of reported transactions

If you report a transaction	FRS takes the following action
0-90 days from the Transaction Date	Accepts the transaction: <ul style="list-style-type: none"> ■ Adds the transaction to the Fraud Master File
91+ days from the Transaction Date	Accepts the transaction, but sends a warning: <ul style="list-style-type: none"> ■ Adds the transaction to the Fraud Master File ■ Flags it as late ■ Lists it on the Warning Activity Report with a Warning Status Code of W20 - Purchase Date

Note If you report a transaction late, this may affect the eligibility of the transaction for acceptance by various Visa Europe programmes, such as the Visa Fraud Monitoring Programme (VFMP) and chargeback rights.

19.3.2 Checking the status of reported fraud transactions

When you submit a fraud transaction, the FRS applies edits to verify that the data in all fields complies with the editing requirements listed in the *Fraud Reporting System (FRS) User's Guide*, and was submitted correctly. It then generates a fraud report that enables you to check the status of your reporting.

The frequency with which you receive these reports and their format depends upon the report options selected when FRS is set up. The default report options are:

- **For Issuers:** Weekly print image reports (TC 45s)
- **For Acquirers:** Fortnightly print image reports (TC 45s)

For a list of all the available report options, see [Report options](#) on the next page. To change your report options, contact Visa Europe Customer Support.

19.3.2.1 Report options

Members that use TC 40 Fraud Advice transactions may receive the following FRS report options.

Table 25: FRS report options

Member type	Report type	Reporting period
Issuer	Visa-generated Transaction Response Records (TC 40s)	Daily
	Print image reports (TC 45s)	Daily, weekly (default)
Acquirer	Visa-generated Transaction Response Records (TC 40s)	Daily, weekly, fortnightly
	Print image reports (TC 45s)	Daily, weekly, fortnightly (default)

For examples of TC 40 and TC 45 reports, see the *Fraud Reporting System (FRS) User's Guide*.

The following reports are also available:

- Monthly summary reports
- Quarterly summary reports

Note Members that use SMS and send or receive 9620 Fraud Advice messages have similar report options, but cannot receive daily summary reports.

All transactions submitted during an Issuer's chosen reporting period (see table above) are listed in one of the three Fraud Activity reports (Confirmed, Warning or Reject) and are summarised in the Fraud Summary reports. Acquirers receive Acquirer Merchant Activity reports.

19.3.2.2 Null reports

FRS sends 'null' reports to members that use TC 40s when both the following conditions apply:

- They have reported fraudulent transactions or have had them reported against their acquiring BIN during the last 90 days; and
- FRS has received no fraud advice messages from an Issuer or has nothing to report to an Acquirer during their chosen reporting period

If FRS receives no fraud transactions from a member for 90 days, the Member is sent no further reports until they resume reporting activity.

Members that connect via SMS and use 9620 Fraud Advice messages do not receive null reports.

19.3.3 Correctly submitted fraud transactions

FRS adds correctly submitted fraud transactions to the Fraud Master File and includes them in the Confirmed Fraud Activity Report. If your reported transactions do not appear in this report, they may be listed in either the Warning Fraud Activity Report or the Reject Fraud Activity Report (see *Incorrectly submitted fraud transactions* below).

FRS sometimes adds correctly reported transactions to the Warning report. Reasons for this include:

- The transaction is a full or partial duplicate of a transaction that has already been reported
- The transaction was reported after the 90-day FRS limit

For information on common reporting problems, see the *Fraud Reporting System (FRS) User's Guide*.

19.3.4 Incorrectly submitted fraud transactions

If one or more fields contain data that does not comply with the editing requirements listed in the *Fraud Reporting System (FRS) User's Guide* or was submitted using incorrect procedures, FRS does one of the following:

- **Accepts the transaction**, applies it to the Fraud Master File, but reports the problem in a daily or weekly Warning Fraud Activity Report as requiring review or correction.
- **Note** If you do not correct the problem detailed in the Warning report for transactions with the warning code W21, W22, W23, W80 or W81 within 30 days of the posting date, FRS deletes the transaction from the Fraud Master File.
- **Rejects the transaction**, does not apply it to the Fraud Master File and reports it in the daily or weekly Reject Fraud Activity report.

Before modifying a transaction on the Visa Fraud Master File, Issuers must review the Confirmed Activity reports to confirm that the transaction was added to the Visa Fraud Master File.

If the transaction is not in the Visa Fraud Master File and an Issuer tries to change or delete it, FRS rejects the modification request message with reject status code R83, indicating that it could not find the transaction in the file.

Important Issuers must modify a previously submitted transaction if the data in the fraud transaction has changed, was incorrect, or was incomplete. However, Issuers must not delete fraud transactions just because the transaction was charged back or charged off.

Unless an Issuer receives an R83-File Key, they must correct the transaction and resubmit the fraud advice message using the Notification Code (NC) 3 and the correct sequence number. If an Issuer receives an R83, they must:

- Check that they have supplied the correct file key data (the account number and Account Sequence Number).

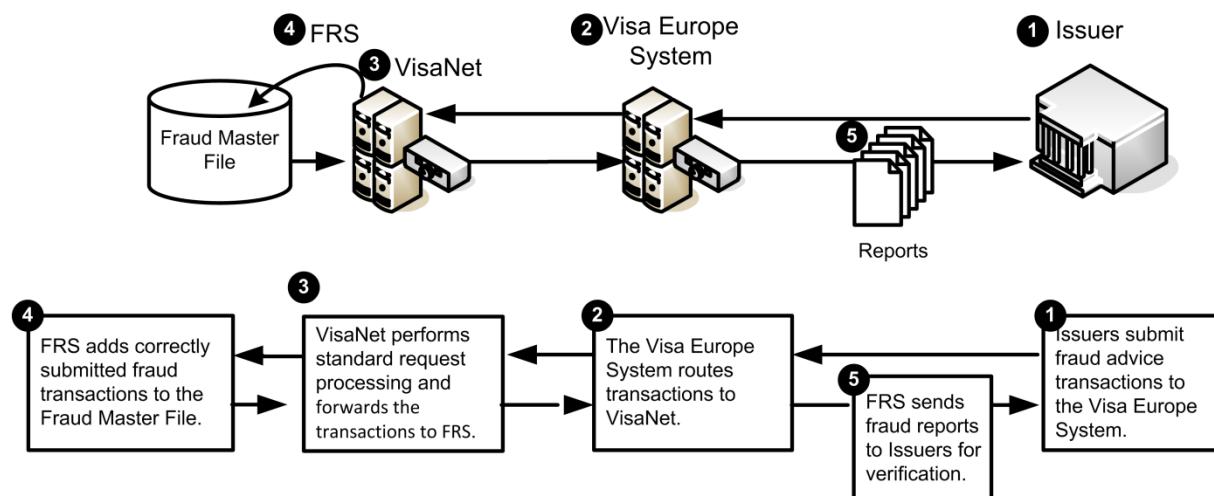
- If they need to change the data in these fields after the transaction has been added to the Fraud Master File, they must delete the incorrect Fraud Master File entry using a fraud advice message with the incorrect key data, and resubmit the fraud advice message with the corrected key data.
- Check that they are not trying to change a transaction that has not been submitted, or delete or reactivate a transaction that has not been added to the Fraud Master File.

For more information on reporting problems, reject codes and resubmitting transactions, see the *Fraud Reporting System (FRS) User's Guide*.

19.4 Process flows

The following diagram gives a simplified view of the process flow for FRS.

Figure 40: Process flow for the FRS



Note Very rarely, Acquirers may also submit fraud advice messages (that is, in the case of Acquirer-reported counterfeit).

For more information about the reporting process, see the *Fraud Reporting System (FRS) User's Guide*.

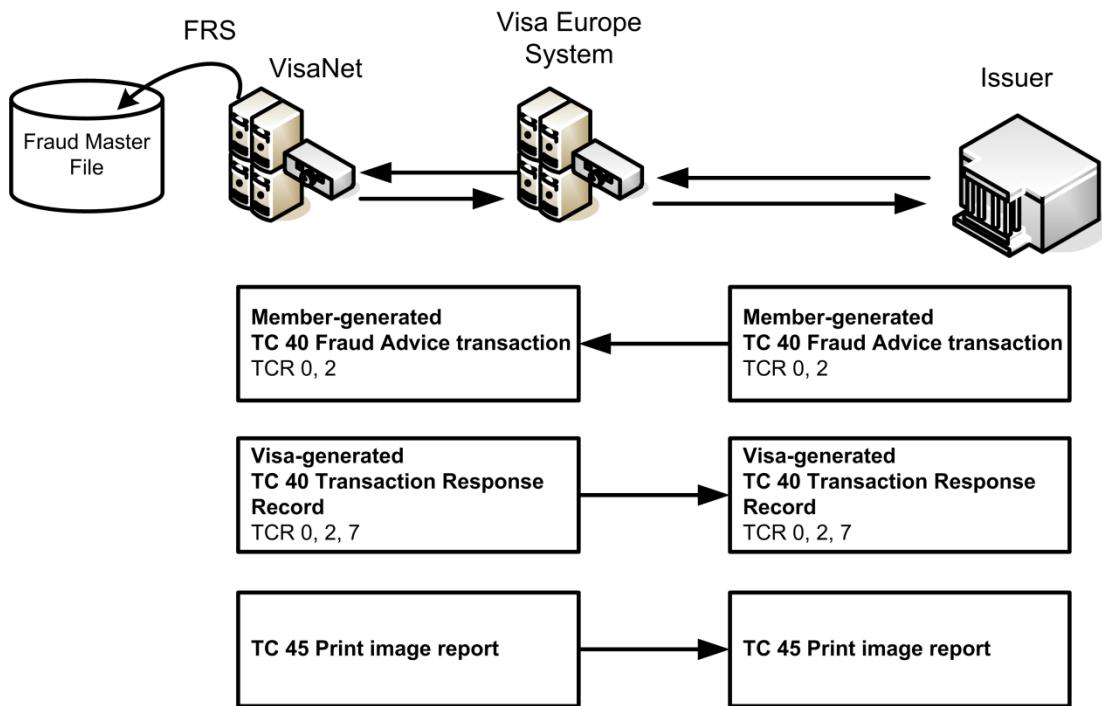
19.5 Message flows

The message flow for FRS depends on whether you send TC 40s or 9620 Fraud Advice messages.

19.5.1 Message flow for Members that send TC 40 Fraud Advice transactions

The message flow for FRS for Members that send TC 40 Fraud Advice transactions is illustrated in the following diagram. Members that send TC 40 Fraud Advice transactions are Members that use dual message processing and Members that use SMS and choose to send TC 40s.

Figure 41: Message flow for Members that send TC 40 Fraud Advice transactions



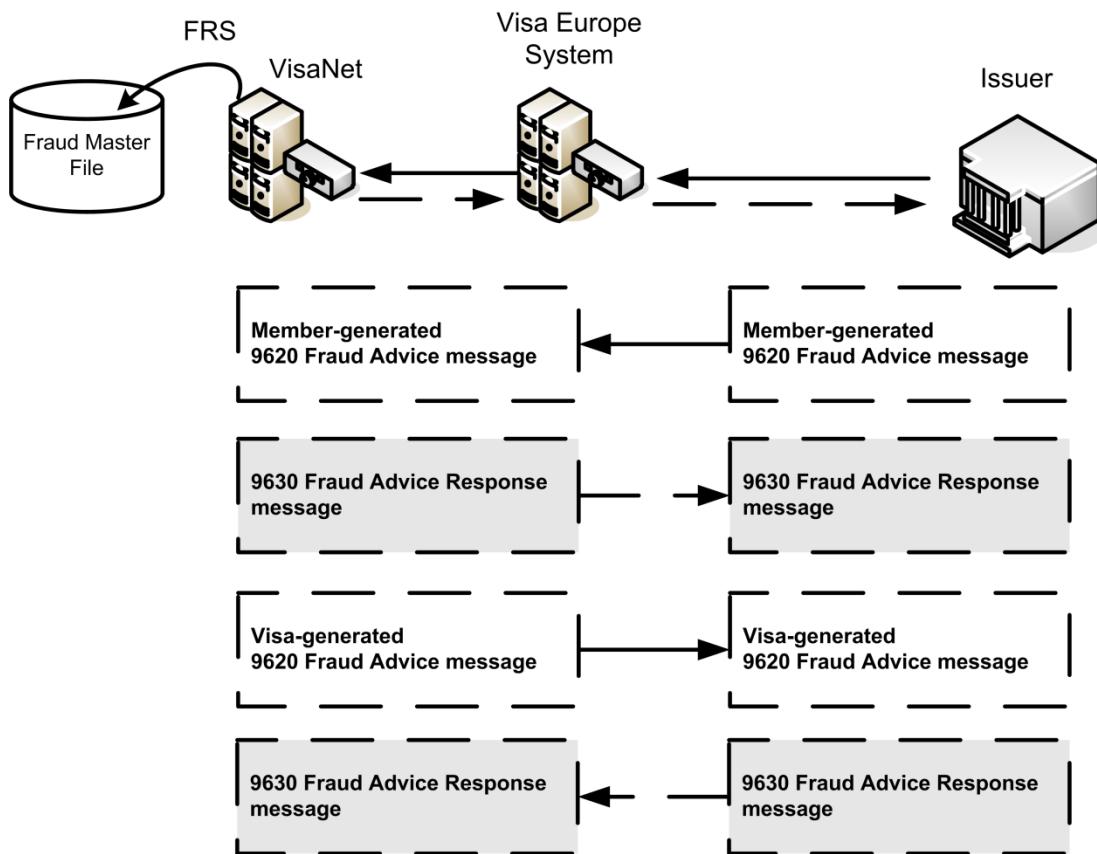
The sequence in which the messages are sent is:

1. Members report confirmed fraud transactions as TC 40 - Fraud Advice transactions to VisaNet via the Visa Europe System. VisaNet holds the messages until end-of-day processing and then forwards them to FRS.
 2. Members receive response messages from FRS as incoming Interchange TC 40 Transaction Response Records and/or TC 45 print image reports.
- If FRS detects discrepancies in the reported fraud data, the Visa-generated TC 40 or TC 45 contains warning or reject information and the Member may have to resubmit the TC 40 Fraud Advice transaction.

19.5.2 Message flow for Members that send 9620 Fraud Advice messages

For Members that use SMS and send 9620 Fraud Advice messages, the flow for FRS is illustrated in the following diagram.

Figure 42: Message flow for Members that send 9620 Fraud Advice messages



The sequence in which the messages are sent is:

1. Members report confirmed fraud transactions using 9620 Fraud Advice messages to VisaNet via the Visa Europe System.
 2. When the Single Message System receives a 9620 Fraud Advice message, it immediately generates a 9630 Fraud Advice Response message that acknowledges receipt of the Member-generated 9620.
 - FRS processes the Member-generated 9620 Fraud Advice message and validates the data received from the Member.
 3. Within 48 hours of receipt of the Member-generated 9620 message, FRS returns to the Member print-image reports via VECSS or a Visa-generated 9620 Fraud Advice message, showing the status of the Member-generated 9620. Members that use VROL for fraud reporting can view the status of reported fraud transactions in VROL.
 4. If the Member has chosen to receive 9620 Fraud Advice messages, they immediately acknowledge receipt of the Visa-generated 9620 message by returning a 9630 Fraud Advice Response message.
- If FRS detects discrepancies in the reported fraud data, the Visa-generated 9620 Fraud Advice message contains warning or error information and the Member may have to resubmit their 9620 message.

Note The Visa-generated 9620 Fraud Advice messages are optional. Members that choose not to receive the Visa-generated 9620 message receive their status information as print-image reports.

19.6 Key messages

Fraud advice messages and their responses transmit information about fraudulent transactions to and from Members:

- Members that use dual message processing send TC 40s
- Members that use SMS may choose to send either TC 40s or 9620s

TC 40 - Fraud Advice transactions

For transactions in Visa Europe, the Member-generated TC 40 comprises two transaction component records (TCRs):

- **TCR 0**

TCR 0 is used primarily for reporting confirmed fraud transactions. Certain fields of this TCR must be completed when reporting mailing information.

- **TCR 2**

TCR 2 is used when reporting confirmed fraud transactions and to report additional information about a fraud transaction.

Visa-generated TC 40s also include an additional TCR:

- **TCR 7**

TCR 7 is used in Visa-generated TC 40 transactions to list the relevant Reject or Warning Status Codes for the returned transaction.

9620 - Fraud Advice messages

Issuers and Acquirers that use SMS use this message to report confirmed fraud transaction messages online.

Optionally, Members may choose to receive Visa-generated 9620 Fraud Advice status messages.

9630 - Fraud Advice Response messages

SMS sends 9630 Fraud Advice Response messages in response to 9620 Fraud Advice messages sent by Issuers or Acquirers.

Members acknowledge receipt of a Visa-generated 9620 Fraud Advice status message by responding with a 9630 Fraud Advice Response message.

For a list of all of the elements in Fraud Advice messages and a field-by-field description of the reporting requirements, see the *Fraud Reporting System (FRS) User's Guide*.

20 Interchange Reimbursement Fee Processing Service

Interchange Reimbursement Fees and Cash Disbursement Fees are paid by Members to each other for transactions entered into Interchange (and their reversals).

The Interchange Reimbursement Fee Processing Service transfers these fees between Members. Visa Europe calculates the fees as part of the daily settlement process.

20.1 Enhanced Interchange Data Service

The Enhanced Interchange Data Service is an additional optional service that enables Issuers to have the fee amount and applicable exchange rate for each transaction automatically calculated and included in clearing transactions they receive from the Visa Europe Clearing and Settlement Service (VECSS).

Issuers that participate in this service do not have to replicate fee edits, derive the exchange rate or calculate fee amounts for each transaction.

20.2 Related information

For further information about the Interchange Reimbursement Fee Processing Service, see the following:

- *Visa Europe Fee Guide*
- *Dual Message System Clearing (DMSC) Technical Specifications*
- *Visa Europe Merchant Data Standards Manual*
- For Interchange Reimbursement Fee levels, click the *Interchange fees* link on the Visa Europe web site: www.visaeurope.com
- For rates and qualification criteria for each jurisdiction, see the applicable *Visa Europe Interchange Reimbursement Fees, Cash Disbursement Fees and Qualification Criteria Guides* available on Visa Online at www.visaonline.com

20.3 Participation

All Members participate in the Interchange Reimbursement Fee Processing Service. Before proceeding, Members should familiarise themselves with the relevant qualification criteria for their jurisdiction.

For information about rates and qualification criteria for each jurisdiction, see the applicable *Visa Europe Interchange Reimbursement Fees, Cash Disbursement Fees and Qualification Criteria Guides* available on Visa Online.

20.4 How the service works

The direction in which fees flow depends on the type of transaction involved:

- For point-of-sale (POS) transactions, Interchange Reimbursement Fees are generally paid by the Acquirer to the Issuer
- For ATM Transactions, Cash Disbursement Fees are generally paid by the Issuer to the Acquirer

Interchange Reimbursement Fees are either a percentage of the transaction value or a flat fee per transaction (or a mixture of both).

The main steps in the Interchange Reimbursement Fee Processing Service in a standard POS transaction where an Acquirer pays an Issuer are:

1. For each clearing transaction, VECSS determines:

- The Merchant's country code and the jurisdiction from the BIN or card range, which indicate the Issuer's country.

The following table shows how the use of a Greek-issued card in various Merchant locations worldwide affects the jurisdiction of the transaction:

Table 26: How jurisdiction of a transaction is determined

Issuer Home Country	Merchant location	Acquirer Home Country	Jurisdiction of transaction
Greece	Greece	Greece	Greek domestic
Greece	Greece	Britain	Greek domestic (where the Acquirer has passported its licence to operate in Greece)
Greece	Spain	Spain	Visa Europe
Greece	Spain	Britain	Visa Europe (where the Acquirer has passported its licence to operate in Spain)
Greece	Japan	Japan	International

- **Applicable card type** from the BIN and card type (such as consumer, commercial, debit or credit).
- **Transaction type** from the information submitted by the Acquirer in the clearing record (such as Cardholder present, Merchant-authorized, system-generated or administrative).
2. Using the above information, together with details from the clearing record sent by the Acquirer, and other elements, such as the timeliness of the transaction (clearing within a certain time period), VECSS calculates and settles the Interchange Reimbursement Fee.
3. The Interchange Reimbursement Fee is credited to the Issuer during settlement.

Note To obtain a particular fee, all qualification criteria must be met exactly. When the criteria are not met VECSS can either downgrade (reclassify) or return transactions, as chosen by the Acquirer. If a transaction is reclassified, VECSS sends a TC 04 message

to the Acquirer, explaining the reason for the reclassification. If a transaction is returned, typically as a TC 01, the Acquirer must review the qualification criteria and re-submit the transaction for clearing.

The Visa Europe Settlement Service (VSS) sends the following settlement reports, which contain information about the Interchange Reimbursement Fee Processing Service:

- VSS-130 Reimbursement Fees Report
- VSS-130-M Monthly Reimbursement Fees Report

20.4.1 Enhanced Interchange Data Service

The Enhanced Interchange Data Service is an optional service. With this service, all TC x5-, TC x6- and TC x7-series clearing transactions that Issuers receive from VECSS include the Interchange Reimbursement Fee and the exchange rate that was applied to the transaction.

Visa Europe provides the calculated Interchange Reimbursement Fee in VECSS Clearing transactions to assist the reconciliation process that Issuers can perform to determine Interchange Reimbursement Fee amounts at transaction level. Issuers do not have to replicate fee edits, derive the rate or calculate Interchange fee amounts for each transaction.

For information on how to subscribe to this service, contact Visa Europe Customer Support.

20.4.1.1 Key data fields used by the Enhanced Interchange Data Service

The following key data fields are used by the Enhanced Interchange Data Service:

TCs x5, x6 and x7 - Draft Data Transactions, TCR 5 - Payment Service Data

For details, see TC 05 Draft Data Transactions in the document *Dual Message System Clearing (DMSC) Technical Specifications*.

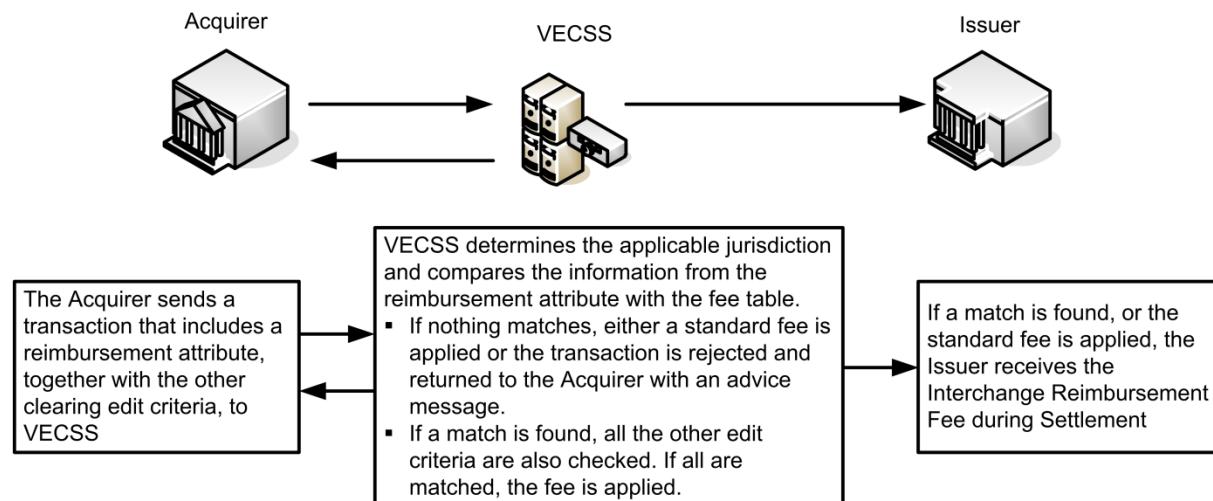
TC 04 - Reclassification Advice Transaction, TCR 9

For details, see TC 04 Reclassification Advice Transaction in the document *Dual Message System Clearing (DMSC) Technical Specifications*.

20.5 Process flow

The following diagram illustrates the process flow for the Interchange Reimbursement Fee Processing Service, showing fees paid from an Acquirer to an Issuer.

Figure 43: Process flow for the Interchange Reimbursement Fee Processing Service



20.6 Key data fields

The following key data fields are used by the Interchange Reimbursement Fee Processing Service:

- Reimbursement Attribute
- POS Terminal Capability
- Authorization Code
- POS Entry Mode
- Cardholder ID Method
- MOTO / ECI indicator
- Merchant Category Code
- POS Environment Code
- Unattended Acceptance Terminal
- Authorization Response Code
- CVV2 Result Code
- EMV Data (TCR 7)
- Tran ID
- Validation Code (TCR 5)
- Request Payment Service Flag (TCR 0)
- ACI
- TCR 3 for commercial cards

For more information on these fields, see the *Dual Message System Clearing (DMSC) Technical Specifications*.

21 International Settlement Service

The International Settlement Service (ISS) is part of the Visa Europe Settlement Service (VSS), which performs settlement for transactions that are cleared through Dual Message System Clearing (DMSC) and the Single Message System (SMS) in a single, centralised service.

ISS is used to settle all International transactions and domestic transactions that do not qualify for National Net Settlement or the Euro Area Net Settlement Service (NNSS or EANSS).

21.1 Related information

For further information about VSS, of which ISS is a part, see the following documents:

- *Visa Europe Settlement Service (VSS) User's Guide*
- *Visa Europe Settlement Funds Transfer Guide*

21.2 Participation

The ISS is available through VECSS. Participation is mandatory for all Members.

21.3 How the service works

The main steps in the ISS are:

1. The Visa Europe System collects Interchange Files containing transactions from Members.
2. DMSC and SMS perform clearing and editing on all transactions.
3. After the close of the Settlement Window, VECSS sends the cleared transactions to VSS.
4. VSS processes the settlement records and delivers:
 - VSS settlement reports that detail the net Settlement Amount to Members' Visa Extended Access Servers (EA Server) on a daily basis.
 - You can use your VSS reports or log into Visa Online to view your settlement position on the Daily Net Settlement Service Positions (DNSSP) page.
 - Funds transfer instructions for Visa Europe Treasury
5. Funds transfer takes place. During this step, funds are paid from Members in a net debit (issuing) position, and paid to Members in a net credit (acquiring) position. When the Member is owed funds, the Settlement Bank of Visa Europe transfers funds to the Member's account at its designated Settlement Bank. When the Member owes funds, the Settlement Bank of Visa Europe sends a request to the Settlement Bank of the Member to transfer funds to the Settlement Bank of Visa Europe.

21.3.1 Clearing and settlement timing

See the *Visa Europe Settlement Service (VSS) User's Guide* for details about the settlement processing schedule for the ISS, including its cut-off time, file delivery time and Settlement Date.

21.3.2 Funds transfer

Funds transfer is the movement of funds between the Settlement Bank of Members and the Settlement Bank of Visa Europe for the purpose of settlement. The funds transferred represent the net position of a Member's credits and debits:

- Members in a net debit (issuing) position pay funds
- Members in a net credit (acquiring) position receive funds

For the Settlement Date on which funds transfer is due, see the *Visa Europe Settlement Service (VSS) User's Guide*. Funds are moved on working days.

21.3.2.1 Paying funds to Visa Europe

Members can choose whether funds they owe are paid manually or are collected via automated drawdown of funds.

Manual payment

Funds paid manually are settled as follows:

1. You determine your settlement position from your VSS reports or from the ISS report section of the DNSSP page on Visa Online.
2. You create a funds transfer from your Settlement Bank to the Settlement Bank of Visa Europe.

Automated drawdowns

The drawdown of funds occurs as follows:

1. Using the SWIFT system, Visa Europe releases a transaction to their Settlement Bank requesting collection of funds from your Settlement Bank.
2. Your Settlement Bank transfers the amount owed to Visa Europe's settlement account.

If you want to set up automated debits (drawdowns), you must ensure your Settlement Bank can accept them and can act on the funds transfer request within the correct settlement timeline for the relevant currency.

USD drawdowns are normally sent before 15:00 GMT (last Sunday in March to last Sunday in October) or 16:00 GMT (rest of the year) each day and are due for settlement on the same day. Your Settlement Bank must therefore be able to acknowledge and complete the transaction at this time. Before settling using drawdowns with Visa Europe, you must complete the Settlement Funds Transfer forms and complete the following steps:

1. Open and fund the account.
2. Set up the account type to receive and process drawdown requests.
3. Grant the authority for Visa Europe to draw down against your settlement account.

An FTSRE can only have funds transferred to or from a single settlement account. However, if a Member has several FTSREs that belong to different settlement services, each FTSRE can use the same account or use different accounts.

Funds transfer amounts can be settled in any of the Settlement Currencies offered by Visa Europe. For further information about the funds transfer process and Settlement Currencies, including a list of those offered by Visa Europe, see the *Visa Europe Settlement Funds Transfer Guide*.

Note Settlement timelines are sometimes adjusted, for example, due to currency holidays.

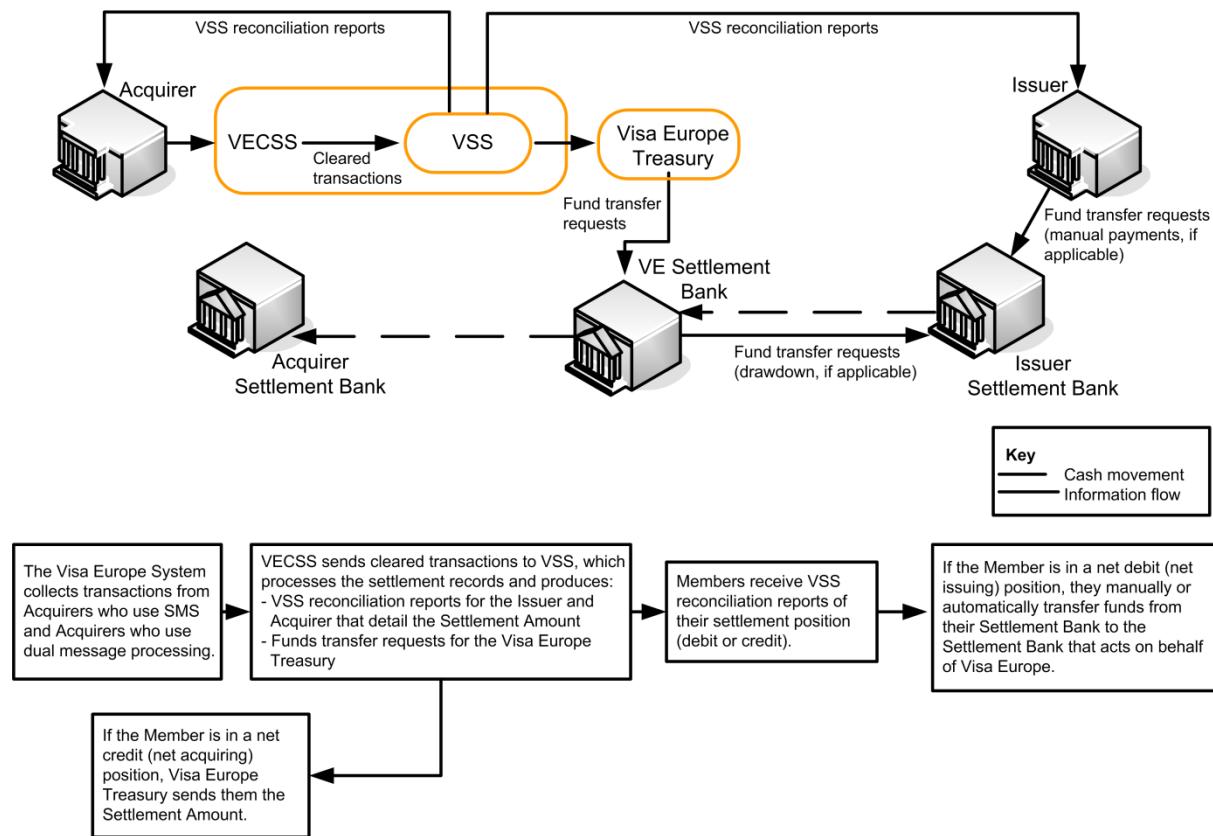
21.3.2.2 Receiving funds from Visa Europe

The Visa Europe Treasury forwards the amount owed to Members that are in a credit position.

21.4 Process flow

The following diagram illustrates the process flow for the ISS.

Figure 44: Process flow for the International Settlement Service



22 Multicurrency Service

The Multicurrency Service enables Members to authorize and clear transactions in most currencies recognised by the International Organization for Standardization (ISO) and supports settlement in a number of international currencies (for an up-to-date list of international currencies, contact Visa Europe Customer Support).

The maximum value for a multicurrency transaction varies between card products, and also depends on whether the transaction is POS, ATM or a manual cash disbursement. The maximum value ranges from the local currency equivalent of USD 99,999.99 to USD 999,999.99. For more information, contact Visa Europe Customer Support.

The Multicurrency Service includes the following Transaction Currency processing features:

- **Authorization/Clearing conversion:** Automatically converts the Transaction Currency to the Billing Currency of the Cardholder. The Transaction Currency is generally the currency in which a transaction takes place. The Billing Currency of the Cardholder is usually the currency of the country in which the account is domiciled. The Visa Europe System supports most currencies that are recognised by the ISO.
- **Settlement conversion:** Automatically converts the Transaction Currency to the Settlement Currency of the Acquirer (if the two are different) and to the Settlement Currency of the Issuer (if the two are different). The Multicurrency Service supports a number of Settlement Currencies.

Members can also subscribe to several related optional services:

- **Currency Rate Delivery Service:** Provides Members (five days a week, Tuesday to Saturday) with the Currency Conversion Rates (in TC 56 format) that Visa Europe uses to process transactions.
For more information, see [Currency Rate Delivery Service](#) on page 188.
- **Enhanced Interchange Data Service:** Participating Issuers automatically receive the Interchange Reimbursement Fee amounts and applicable Currency Conversion Rate in each clearing transaction sent to them by the Visa Europe Clearing and Settlement Service (VECSS).
For more information, see [Enhanced Interchange Data Service](#) on page 188.
- **Currency Precision Service:** This service is only available to users of the Multicurrency Service that also use the Single Message System (SMS). This service uses field 63.13 - Decimal Positions Indicator to indicate how many decimal positions are in the message amount fields.
For more information, see [Currency Precision Service](#) on page 184.

22.1 Related information

For further information about the Multicurrency Service, see the following documents:

- [Single Message System \(SMS\) POS Technical Specifications](#)
- [Single Message System \(SMS\) ATM Technical Specifications](#)

- *Dual Message System Authorization (DMSA) Technical Specifications*
- *Dual Message System Clearing (DMSC) Technical Specifications*
- *Visa Europe Settlement Funds Transfer Guide*
- *Dynamic Currency Conversion (DCC) Acquirer and Merchant Standards Manual*

For further information regarding the implementation of this service, contact Visa Europe Customer Support.

22.2 Participation

Participation in the Multicurrency Service is mandatory for all Members.

22.3 How the service works

The main steps in the Multicurrency Service are:

1. The Acquirer sends an authorization request that indicates the Transaction Currency used at the point-of-sale or ATM to VEAS.

Dynamic Currency Conversion (DCC)

If the Acquirer and Merchant or ATM owner use DCC, the Cardholder may be given the choice of having the purchase price of goods or services converted to their Billing Currency before the transaction is submitted for authorization.

For example, a Cardholder who is billed in euros may visit a Merchant whose local currency is Turkish lira. The Merchant offers the Cardholder the choice of using DCC. The Cardholder accepts the option and DCC converts the purchase price in Turkish lira to euros before the transaction is authorized. In this case, the Transaction Currency used at the point-of-sale is the euro.

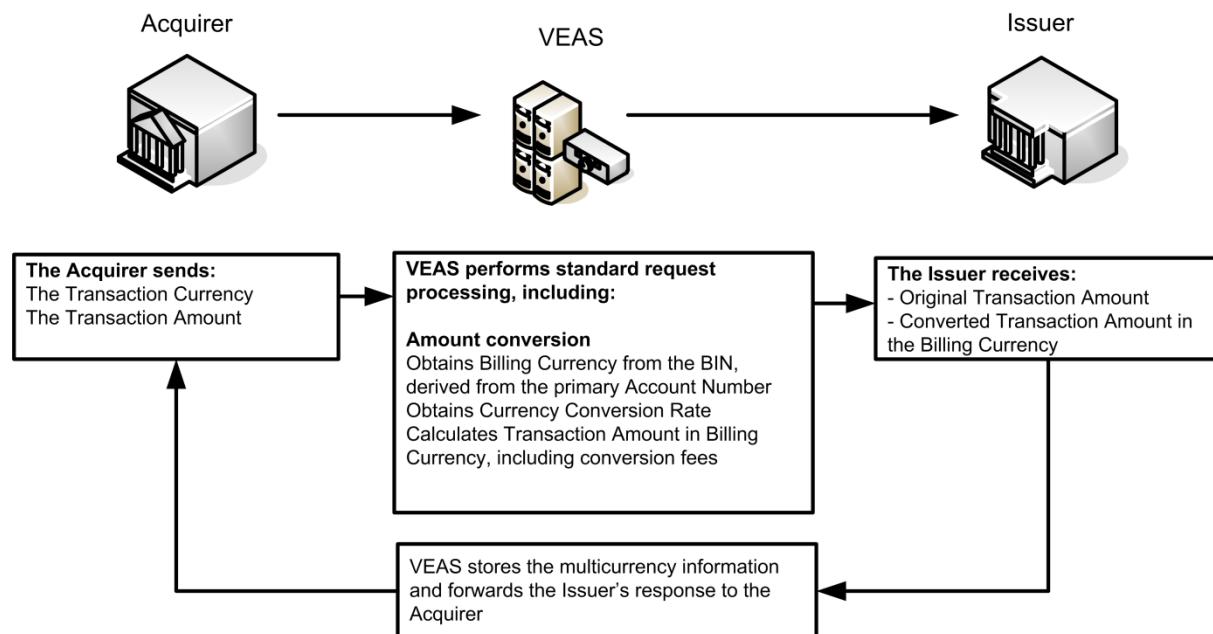
For more information on DCC, see the *Dynamic Currency Conversion (DCC) Acquirer and Merchant Standards Manual*.

2. VEAS determines the Billing Currency from the Issuer parameters, looks up the Currency Conversion Rate between Acquirer and Issuer currencies, checks for any optional Issuer currency conversion fees and makes the conversion to the amount expressed in the Billing Currency of the Issuer. VEAS then routes the authorization request to the Issuer.
3. The Issuer sends the appropriate authorization response to VEAS.
4. VEAS stores the multicurrency information for logging purposes and forwards the Issuer's response to the Acquirer.
 - In the case of SMS processing, VEAS also includes - for Issuer and/or Acquirer - the Settlement Amount in the request/response messages.
 - The Acquirer will only receive field 6 - Amount, Cardholder Billing when the value in field 39 - Response Code is either 01 (refer to card issuer) or 02 (refer card to issuer, special condition).
5. The Acquirer submits the transaction to VECSS in the currency that is used at the point-of-sale or ATM.

6. The Visa Europe System performs standard clearing processing and currency conversion.
7. The Visa Europe System routes the transaction to the Issuer. Both the Acquirer and Issuer can choose to settle in any supported Settlement Currency.

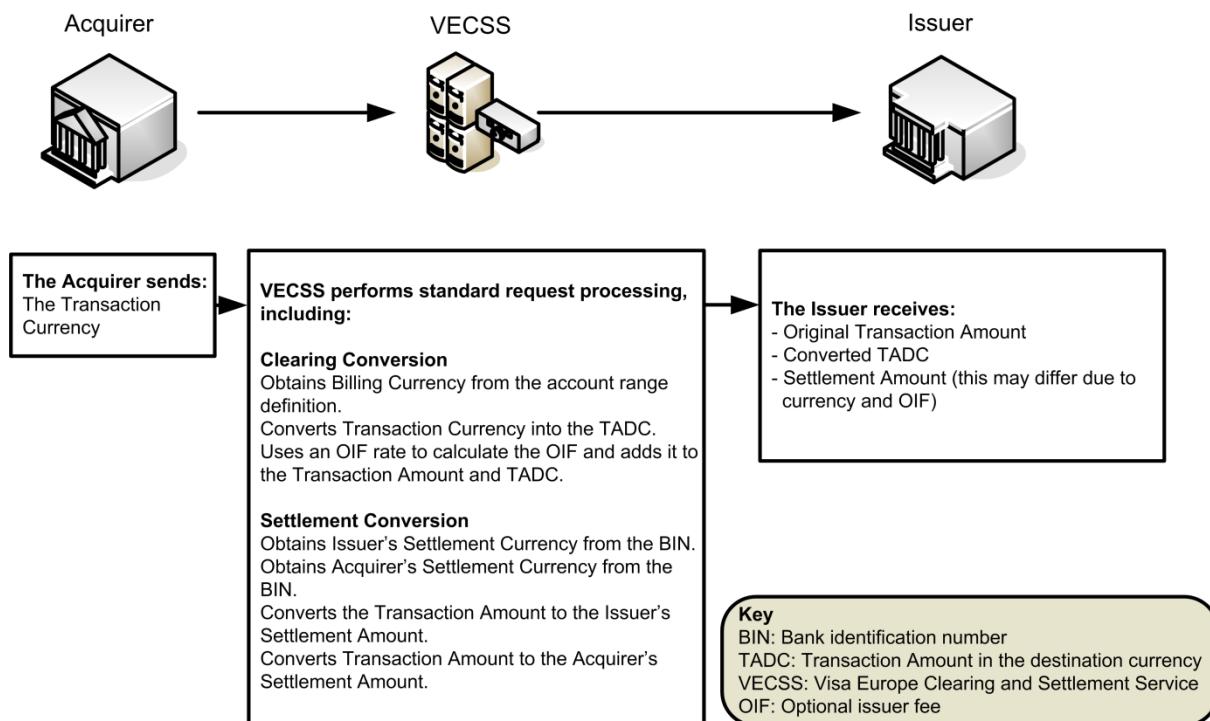
The following diagram illustrates the principle of authorizing a multicurrency purchase transaction.

Figure 45: Authorizing a multicurrency transaction



The service automatically converts the net financial position into any of the predetermined currencies supported by the International Settlement Service.

The following diagram illustrates the principle of clearing and settling a transaction.

Figure 46: Clearing and settling a multicurrency transaction

Note The Optional Issuer Fee (OIF) is not included in the Settlement Amount but is just added to the Transaction Amount in destination currency (TADC). For an explanation of TADC and other terms relating to currency conversion, see [Understanding rate-related terminology](#) on page 179.

22.3.1 Visa Europe System acquired MasterCard transactions

MasterCard transactions can also be submitted in any currency valid in the Visa Europe System. Any currency conversion necessary will be performed by the MasterCard system once the transaction has been routed to MasterCard.

Note that referrals on Visa cards will contain the converted billing amount (in field 6), currency (in field 51) and conversion rate (in field 10) in the response to the Acquirer. However, in referral responses for MasterCard authorizations, these fields are not supplied.

22.3.2 Understanding decimal positioning

Currencies are defined as having zero, two or three minor units of currency. For example, the euro has two minor units of currency (the two positions to the right of the decimal point); the Japanese yen has no minor units. VEAS takes implied decimals into account in its processing; however, the Visa Europe Clearing and Settlement Service (VECSS) always assumes two minor units for reporting purposes and settlement calculations.

Participants using a currency with three decimal places must configure their systems to replace the third decimal position with zero when generating amount fields. However, this requirement does not apply to SMS Currency Precision Service participants, who can override the number of minor units.

For a list of countries, currencies and their minor units, see the Visa Europe technical specifications manuals. The following table gives examples of decimal positioning.

Table 27: Examples of decimal positioning

Transaction Amount	No. of decimal positions in rate table	It is entered in the transaction or request message as		
		DMSC	VEAS / SMS	Currency Precision Service (SMS)
500000	0	50000000	500000	
20492	2	2049200	2049200	
67.89	2	6789	6789	
3.129	2	313	313	
3.129	3	313	3129	
12.34	2	1234	1234	03 decimals 12340
123.450	3	12345	123450	02 decimals 12345

22.3.3 How currency conversions are calculated

The Visa Europe System uses two components to convert currencies:

- A buy and/or sell rate (see [Currency conversion rate pairs](#) below) to obtain the Transaction Amount in destination currency (TADC). For information on how these rates are applied, see [How buy and sell currency rates are applied to transactions](#) on the next page.
- The optional issuer fee (OIF), if any (see [Charging an Optional Issuer Fee](#) below) for sales drafts, credit vouchers, cash advances and their reversals.

The sum of TADC and OIF is carried in the Destination Amount field.

22.3.3.1 Currency conversion rate pairs

Visa Europe uses buy and sell rates determined from rates available on currency markets for currency conversion. These rates are paired into:

- USD-based rates that are used when converting non-USD currencies against the US dollar.
- Cross rates (non-USD-based rates) that are used for selected currencies for which the rates quoted are against a currency other than the US dollar. The cross rates that the Visa Europe System uses are available on request.

22.3.4 Charging an Optional Issuer Fee

Issuers can choose to charge an Optional Issuer Fee (OIF), which is a percentage rate established by the Issuer, to the Cardholder for transactions that require currency conversion. The Issuer can specify a Visa Europe OIF or international OIF, or both.

The OIF, which may be positive or negative, is maintained in the Visa Europe System databases according to the Issuer's BINs or account range. OIFs applied at the account range level take precedence over those applied at the BIN level. This optional fee is calculated at conversion time, using the percentage rate established by the Issuer. It is included in field 6 - Cardholder Billing Amount. To modify an existing OIF, contact Visa Europe Customer Support.

Issuers that use SMS may optionally receive the OIF as a discrete value as part of the online financial message (field 63.14 - Issuer Currency Conversion Data).

Note The OIF is not included in the Settlement Amount but is just added to the Transaction Amount in destination currency (TADC).

All Visa Europe systems that support Multicurrency Service processing use common conversion rates.

22.3.5 Choosing the Settlement Currency

The service automatically converts your net financial position into any of the currencies supported by the International Settlement Service. You can choose to settle in any of the supported Settlement Currencies. For further information about Settlement Currencies, including a list of those offered by Visa Europe, see the *Visa Europe Settlement Funds Transfer Guide*.

22.4 How buy and sell currency rates are applied to transactions

This section describes how Visa Europe Clearing and Settlement Service (VECSS) applies buy and sell rates to transactions during clearing and settlement.

22.4.1 Understanding rate-related terminology

Visa Europe's Currency Conversion Rate system involves specific terminology as defined in the following table.

Table 28: Rate-related terminology

Term	Description
Base currency	Variable units of a base currency are equivalent to one unit of a counter currency
Counter currency	One unit of a counter currency is equivalent to variable units of a base currency
Buy rate	The number of units of base currency required to buy one unit of the counter currency
Sell rate	The number of units of base currency received from selling one unit of the counter currency

Table 28: Rate-related terminology (continued)

Term	Description
USD-based rate pair	A rate pair in which the US dollar is always the base currency. The rate expresses a variable number of US dollars for each unit of the counter currency. The counter currency will be a currency other than USD.
Non-USD-based rate (cross rate) pair	A rate pair in which the rate quoted is between two currencies, neither of which is the US dollar. Such rates are applied only when the currencies of the cross rate pair are the only currencies between the source amount and the Transaction Amount in destination currency (TADC). Rates are expressed as a variable number of base currency per unit of counter currency.
Triangulation	Triangulation occurs when no cross rate exists between a non-USD-based rate pair. In this situation the source amount is converted into USD and then the USD is converted into the TADC.
Exchange direction	The set of currency conversion calculations that are applied to a transaction, based on the transaction type
Transaction Amount in destination currency (TADC)	The submitted Transaction Amount in the currency that is appropriate to the destination endpoint. The TADC is included in the Destination Amount field. In addition to the TADC, the Destination Amount field may contain the OIF (see Charging an Optional Issuer Fee on page 178. The Destination Amount field is provided in clearing transactions to the destination Member. Issuers have the discretion to increase or decrease the amount in this data field when billing Cardholders.

The following table provides a mapping of the terminology used in the above table with the corresponding fields in a DMSC message, as described in the *Dual Message Clearing (DMSC) Technical Specifications* manual.

Table 29: Mapping of rate-related terms to fields in DMSC messages

Term	DMSA, SMS field name	VECSS TCR/Position
Source amount	4 - Amount, Transaction	Draft Data TCR 0, Positions 77-88
TADC (in Destination Amount field)	6 - Amount, Cardholder Billing	Draft Data TCR 0, Positions 62-73 Note In the <i>Dual Message Clearing (DMSC) Technical Specifications</i> manual, only the TADC component is described and displayed in these fields. The OIF and currency conversion charge are not addressed.
Settlement amount, Acquirer or Issuer	5 - Amount, Settlement (SMS only)	n/a

22.4.2 How rate pairs are determined

When converting currencies, the Visa Europe System compares the source currency and the destination currency to determine whether to use a USD-based or a non-USD-based rate pair for a transaction.

The Visa Europe System applies the USD-based rates to all settlement services and to all amounts, including assessments and charges that are displayed on daily settlement reports, except when **all** of following conditions are met. In this case, a non-USD-based rate is applied:

- The source amount and the TADC are in different non-USD currencies and a non-USD-based rate pair exists
- A non-USD-based rate pair (for example, euros to pounds sterling) was used to calculate the TADC
- A non-USD-based rate exists that matches the currencies of the source amount and the specified Settlement Amount, either source Settlement Amount or destination Settlement Amount

The Visa Europe System applies USD-based rates to transactions when a match between the currencies in the transaction and a corresponding non-USD-based rate pair is not found on the Rate File (the currency rates file distributed by Visa Europe to Members on request).

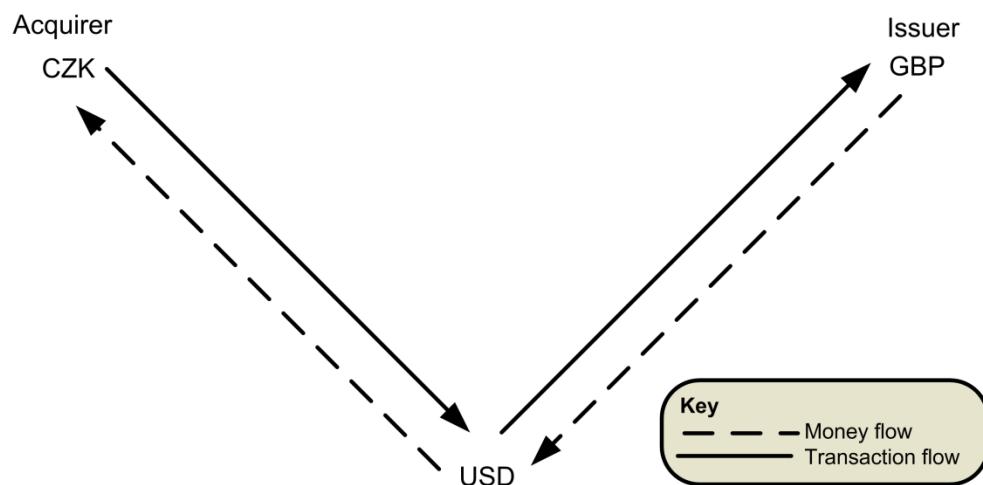
22.4.3 How buy and sell rates are applied

After the Visa Europe System has established the rate pairing type (see *How rate pairs are determined* above) it determines which rate (buy or sell) within the pair to apply to the transaction, based on what is happening to the counter currency. If more than one conversion is required, both a buy rate and a sell rate can be applied in the same transaction. This is the case when converting between currencies for which no direct exchange rate is available. Under these circumstances, US dollars (USD) are used for conversion.

For example, for a transaction where a UK Cardholder uses their card in the Czech Republic, pounds sterling (GBP) must be converted to Czech koruna (CZK). As there is no direct exchange rate, Visa Europe sells the GBP and buys USD, then sells USD and buys CZK.

Note Although the transaction flow is from Acquirer to Issuer, the money flows from Issuer to Acquirer.

The process of converting from one currency to another via a third currency is known as triangulation. The following diagram illustrates the transaction flow from Acquirer to Issuer.

Figure 47: Triangulation - Acquirer to Issuer

The following are the basic formulae that the Visa Europe System uses for all transactions when converting currencies.

When converting from	The formula is
Counter currency to base currency	Amount in counter currency x rate = Amount in base currency
Base currency to counter currency	Amount in base currency ÷ rate = Amount in counter currency

From these basic formulae, Visa Europe has established calculations for each type of transaction and has categorised them into the following exchange direction groupings:

- **Buy:** Used when a cross rate is involved or where USD are the source or destination
- **Sell:** Used when a cross rate is involved or where USD are the source or destination
- **Buy-Sell:** Used when a triangulated rate is involved
- **Sell-Buy:** Used when a triangulated rate is involved

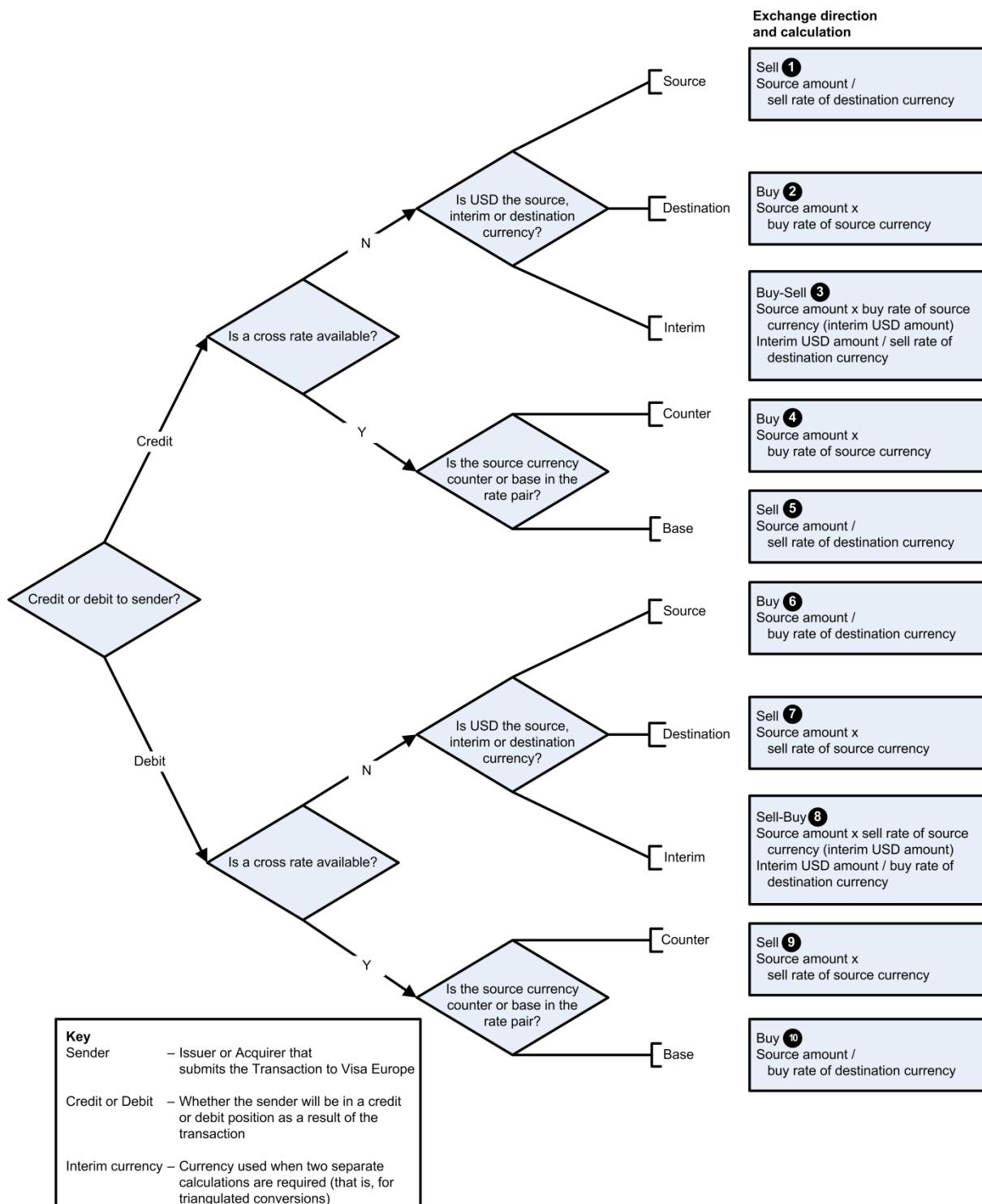
The Visa Europe System uses exchange direction calculations for the rate pair type that is appropriate for the transaction and for the type of conversion required when converting the currency.

For a brief summary of how Visa Europe converts currency, with examples, see [Currency conversion process in brief](#) below.

22.5 Currency conversion process in brief

The following decision tree shows how the Visa Europe System determines the type of conversion that is required to convert a source amount to a TADC.

Figure 48: Conversion of TADC to destination currency



Note This diagram shows the rates applied in TC 56 reports.

22.5.1 Examples of currency conversions

The following table shows examples of each of the preceding calculations applied to currency rate conversions. The **No.** column indicates the relevant calculation from the diagram.

Table 30: Examples of currency conversions

No.	Source Currency	Source Amount	Destination Currency	Rate pair(s)	Rates (Buy/Sell)	Destination amount calculation
1	US dollar (USD)	250.00	Danish krone (DKK)	DKK-USD	0.21 / 0.20	USD 250.00 / 0.20 = DKK 1,250.00
2	Moldovan leu (MDL)	500.00	US dollar (USD)	MDL-USD	0.0080 / 0.0079	MDL 5000.00 x 0.0080 = USD 40.00
3	Czech koruna (CZK)	300.00	Pound sterling (GBP)	1. CZK-USD 2. GBP-USD	1. 0.050 / 0.049 2. 1.51 / 1.50	1. CZK 300.00 x 0.050 = USD 15.00 2. USD 15.00 / 1.50 = GBP 10.00
4	Swiss franc (CHF)	400.00	Euro (EUR)	CHF-EUR	0.75 / 0.74	CHF 400.00 x 0.75 = EUR 300.00
5	Euro (EUR)	200.00	Polish zloty (PLN)	PLN-EUR	0.26 / 0.25	EUR 200.00 / 0.25 = PLN 800.00
6	US dollar (USD)	80.00	Moldovan leu (MDL)	MDL-USD	0.0080 / 0.0079	USD 80.00 / 0.0080 = MDL 10,000.00
7	Danish krone (DKK)	500.00	US dollar (USD)	DKK-USD	0.21 / 0.20	DKK 500.00 x 0.20 = USD 100.00
8	Pound sterling (GBP)	400.00	Czech koruna (CZK)	1. GBP-USD 2. CZK-USD	1. 1.51 / 1.50 2. 0.050 / 0.049	1. GBP 400.00 x 1.50 = USD 600.00 2. USD 600.00 / 0.050 = CZK 12,000.00
9	Polish zloty (PLN)	350.00	Euro (EUR)	PLN-EUR	0.26 / 0.25	PLN 1,000.00 x 0.25 = EUR 250.00
10	Euro (EUR)	900.00	Swiss franc (CHF)	EUR-CHF	0.75 / 0.74	EUR 900.00 / 0.75 = CHF 1,200.00

In the above table, the first example is of a transaction where the source amount (USD 250.00) is credited to the sender. No cross-rate is involved so a USD-based rate is used. In this transaction, the source currency is USD, so as shown in the decision tree, the exchange direction is Sell. The calculation that applies is source amount (USD 250.00) / the sell rate of destination currency (0.20).

The other examples follow a similar process.

22.6 Currency Precision Service

Users of SMS can optionally participate in the Currency Precision Service. This service uses field 63.13 - Decimal Positions Indicator to indicate the number of decimal positions included in message amount fields. That is, the number of decimal positions will always be

explicitly stated in the SMS message, rather than implicitly derived from the currency rate table.

Field 63.13 allows for separate settings for Transaction Amounts, Settlement Amounts, and Cardholder Bi amounts. An amount type can be set to include zero (00), two (02) or three (03) decimal positions. These values override the number of minor units in the currency rate table. For non-participants, Visa Europe System always uses the values in the currency rate table.

The service is effective in the following message fields.

Table 31: Currency Precision Service - applicable fields

Currency Precision Service				
Affected message field	Field 63.13 - number of decimal positions indicators			
	Transaction Amounts (position 1-2)	Settlement Amounts (position 3-4)	Cardholder amounts (position 5-6)	
4	Amount, transaction	nn		
5	Amount, settlement		nn	
6	Amount, cardholder billing			Nn
54	Additional amounts	nn		
61.1	Other amount, transaction	nn		
61.2	Other amount, cardholder			Nn
86	Credits, amounts		nn	
87	Credits, reversal amount		nn	
88	Debits, amount		nn	
89	Debits, reversal amount		nn	
97	Amount, net settlement		nn	

22.6.1 Currency Precision Service for Acquirers

Acquirers must be able to set the decimal positions indicator in the following transactions and receive the indicator in corresponding responses:

- Authorizations
- Financial requests
- Reversals
- Adjustments
- Representments

Acquirers must be able to receive the decimal positions indicator in the following messages:

- Balance inquiry responses
- Representment status advices
- Chargebacks
- Reconciliation messages

22.6.2 Currency Precision Service for Issuers

Issuers must be able to set the decimal positions indicator in balance inquiry responses. They must also be able to send the indicator in chargebacks. Issuers must be able to receive the decimal positions indicator in the following messages:

- Authorizations
- Financial requests
- Reversals
- Adjustments
- Representments
- Issuer status advices
- Reconciliation messages

22.6.3 One position decimal adjustment

If the number of decimal positions specified in data field 63.13 is less than that in the currency rate table, VEAS adjusts the applicable amount fields.

Example

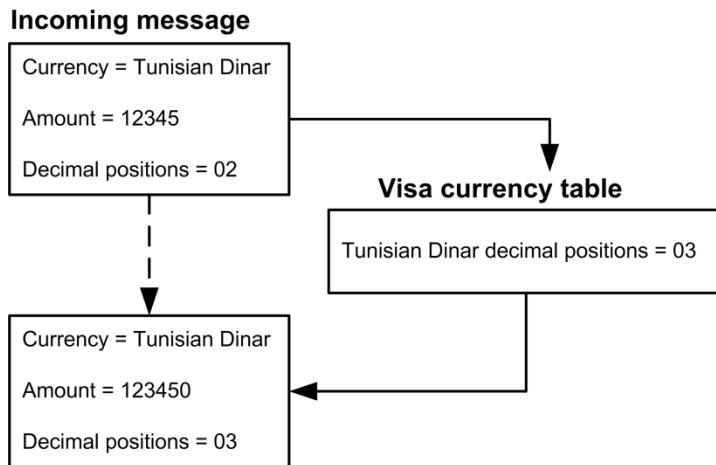
An Acquirer sends a message with a Transaction Amount of 12345 and data field 63.13, indicating two decimal positions. However, the currency rate table indicates that the Acquirer's currency has three decimal positions.

The Issuer receives the Transaction Amount 123450.

A participating Issuer also receives field 63.13 indicating three decimal positions.

A non-participating Issuer receives a Transaction Amount of 123450 in data field 4 - Amount, Transaction. However, the request will have no decimal positions indicator.

The Settlement Amount is based on the Transaction Amount 123450. All reports and raw data reflect the Transaction Amount 123450.



22.6.4 Two position decimal adjustment

If the number of decimal positions specified in data field 63.13 is greater than that in the currency rate table, the last digit, which must be zero, is removed.

Example

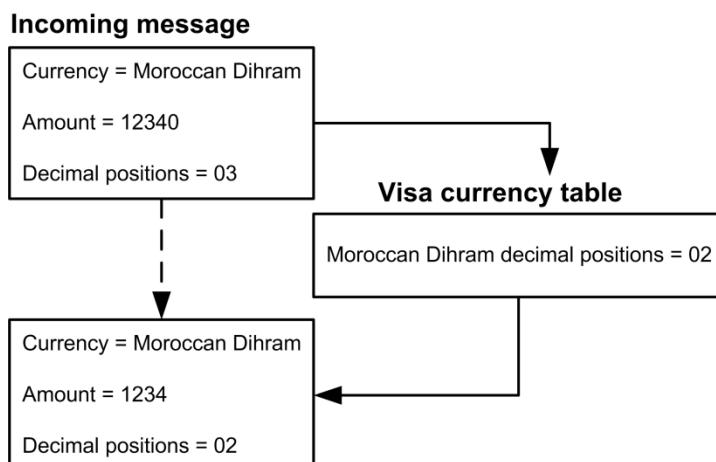
An Acquirer sends a message with a Transaction Amount of 12340 and data field 63.13, indicating three decimal positions. However, the currency rate table indicates that the Acquirer's currency has two decimal positions.

The Issuer receives the Transaction Amount 1234

A participating Issuer also receives data field 63.13, indicating two decimal positions.

A non-participating Issuer receives a Transaction Amount of 1234 in field 4 - Amount, Transaction. However, the request will have no decimal positions indicator.

The Settlement Amount is based on the Transaction Amount 1234. All reports and raw data reflect the Transaction Amount 1234.



22.7 Currency Rate Delivery Service

The Visa Europe System obtains and verifies international currency rates from various sources around the world.

Visa Europe delivers the same Currency Conversion Rate information that it uses to Members and their Processors that subscribe to the Currency Rate Delivery Service. This optional service enables Members to receive rates daily (Tuesday to Saturday) via their clearing files.

The Visa Europe System uses the Currency Conversion Rate Update Records (TC 56) to transmit updates to your conversion rate file.

Each entry contains:

- The ISO numeric currency code of the counter currency
- The ISO numeric currency code of the base currency
- The Visa Interchange Center (VIC) processing date
- The buy conversion and sell conversion rate applied to the currency that day
- The currency scale factor identifier for each of the Currency Conversion Rates

For more details, see the *Dual Message System Clearing (DMSC) Technical Specifications* manual.

For information about how to participate in the Currency Rate Delivery Service, contact Visa Europe Customer Support.

22.8 Enhanced Interchange Data Service

The Enhanced Interchange Data Service is an optional service that enables subscribing Issuers to receive the following values in all TC x5, TC x6 and TC x7 series clearing transactions they receive from VECSS:

- **Interchange Reimbursement Fee**

To assist the reconciliation process that Issuers can perform to determine Interchange Reimbursement Fee amounts, Visa Europe provides the calculated Interchange Reimbursement Fee (IRF) in each clearing transaction that Issuers receive from VECSS. Subscribing Issuers do not have to replicate fee edits or calculate Interchange fee amounts for each transaction.

- **Currency Conversion Rate Information**

Each transaction that an Issuer receives from VECSS includes the Currency Conversion Rate that was applied to the transaction, where applicable. Participating Issuers know precisely the rate that is applied to each transaction and avoid having to reconcile each transaction to exchange rate tables in TC 56s.

For information on how to subscribe to this service, contact Visa Europe Customer Support.

22.8.1 Transaction types used by the Enhanced Interchange Data Service

The following key transaction types are used by the Enhanced Interchange Data Service:

TC 05, 06 and 07 - Draft Data Transactions, TCR 5 - Payment Service Data

- For details, see TC 05 Draft Data Transactions in the *Dual Message System Clearing (DMSC) Technical Specifications* manual.

TC 04 - Reclassification Advice Transaction, TCR 9

- For details, see TC 04 Reclassification Advice Transaction in the *Dual Message System Clearing (DMSC) Technical Specifications* manual.

22.9 VEAS: Key messages for the Multicurrency Service

The following messages are key for the Multicurrency Service.

Dual Message System Authorization and SMS messages:

- 0100 authorization requests
- 0110 authorization responses
- 0120 advices
- 0200 financial requests
- 0210 financial responses
- 0220 financial advices
- 0230 financial advice responses
- 0400 reversal requests/cash disbursement adjustments
- 0420 reversal advices/cash disbursement adjustments
- 0422 chargeback requests and reversals and Issuer's fee collection transactions and fund disbursements
- 0432 chargeback responses
- 0520 reconciliations for Visa and Plus

22.10 VEAS: Key data fields used by the Multicurrency Service

The following key data fields are used by the Multicurrency Service. Unless stated otherwise, data fields are relevant to both Dual Message System Authorization and SMS. For more detailed information, see the Visa Europe technical specifications.

Data field 4 - Amount, Transaction

This data field contains the Transaction Amount in the Transaction Currency of the Acquirer. Issuers receive the Transaction Amount submitted by the Acquirer.

Data field 5 - Amount, Settlement

SMS only

This data field contains the Transaction Amount in field 4 converted to the Settlement Currency of the Issuer/Acquirer. It does not include any OIF.

Data field 6 - Amount, Cardholder Billing

This data field contains the Transaction Amount in field 4 converted to the Billing Currency. It includes the Transaction Amount in destination currency (TADC) and, where applicable, the OIF.

Data field 9 - Conversion Rate, Settlement

SMS only

This data field contains the Currency Conversion Rate used to convert the amount in field 4 converted to the field 5 amount.

Data field 10 - Conversion Rate, Cardholder Billing

This data field contains a calculated value that represents a factor that might be applied to the amount in field 4 to obtain the field 6 amount. It is not the rate that VEAS actually uses for currency conversion.

Data field 16 - Date, Conversion

SMS only

This data field contains the effective date of the field 4 to field 5 currency conversion. It appears only if data field 5 is present.

Data field 49 - Currency Code, Transaction

This data field contains the code that identifies the field 4 currency and the field 61.1 currency.

Data field 50 - Currency Code, Settlement

SMS only

This data field contains the code that identifies the field 5 currency.

Data field 51 - Currency Code, Cardholder Billing

This data field contains the code that identifies the currency in fields 6 and 61.2.

Data field 54 - Additional Amounts

This data field contains account balance information.

Data field 61.1 - Other Amount, Transaction

In a Cash-Back transaction, this data field contains the Cash-Back amount.

Data field 61.2 - Other Amount, Cardholder Billing

This data field contains the field 61.1 amount expressed in the Billing Currency. It includes any appropriate OIF.

Data field 63.13 - Decimal Positions Indicator

SMS currency precision service users only

This data field contains the number of decimal positions in Transaction Amount, Settlement Amount and Cardholder amount fields.

Data field 63.14 - Issuer Currency Conversion Data

SMS issuers only

This data field contains the fees associated with a transaction that undergoes currency conversion.

22.11 DMSC: Key messages and fields used by the Multicurrency Service

The Multicurrency Service affects the following transaction types:

- TC x5, TC x6 and TC x7 - Draft Data Transactions, TCR 0
 - Positions 62-73 - Destination Amount
 - Positions 74-76 - Destination Currency Code
 - Positions 77-88 - Source Amount
 - Positions 89-91 - Source Currency Code
- TC x5, TC x6 and TC x7 - Draft Data Transactions, TCR 5 - Payment Service Data
 - Positions 108-115 - Source Currency to Base Currency Exchange Rate
 - Positions 116-123 - Base Currency to Destination

For detailed information, see the *Dual Message System Clearing (DMSC) Technical Specifications* manual.

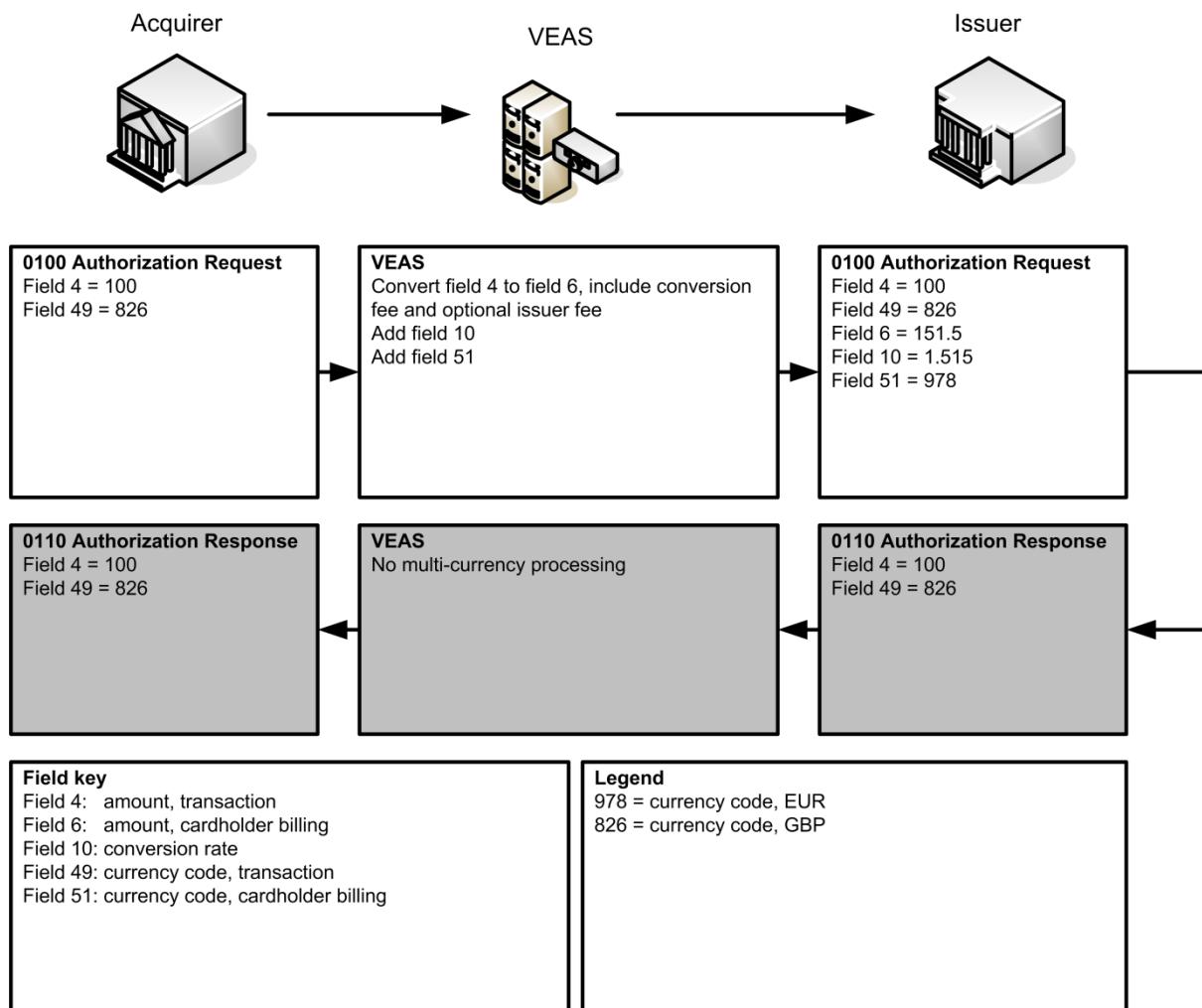
22.12 Multicurrency transaction examples

This section includes a number of example transaction flows that help to illustrate how multicurrency data is managed.

22.12.1 Example 1 - DMSA purchase transaction

In the following example:

- Cardholder account is in pounds sterling (GBP)
- Cardholder purchases an item in France (EUR)
- Currency conversion rate is GBP 1 = EUR 1.5
- Visa conversion fee plus OIF is GBP 1.5

Figure 49: Multicurrency transaction example 1

1. The Acquirer sends a 0100 authorization request to VEAS.
2. VEAS processes the authorization request and forwards it to the Issuer.
The value in field 10 is calculated by dividing the value in field 6 by that in field 4.
3. The Issuer sends a 0110 authorization response.
4. VEAS sends the authorization response back with no further additions to the currency fields.

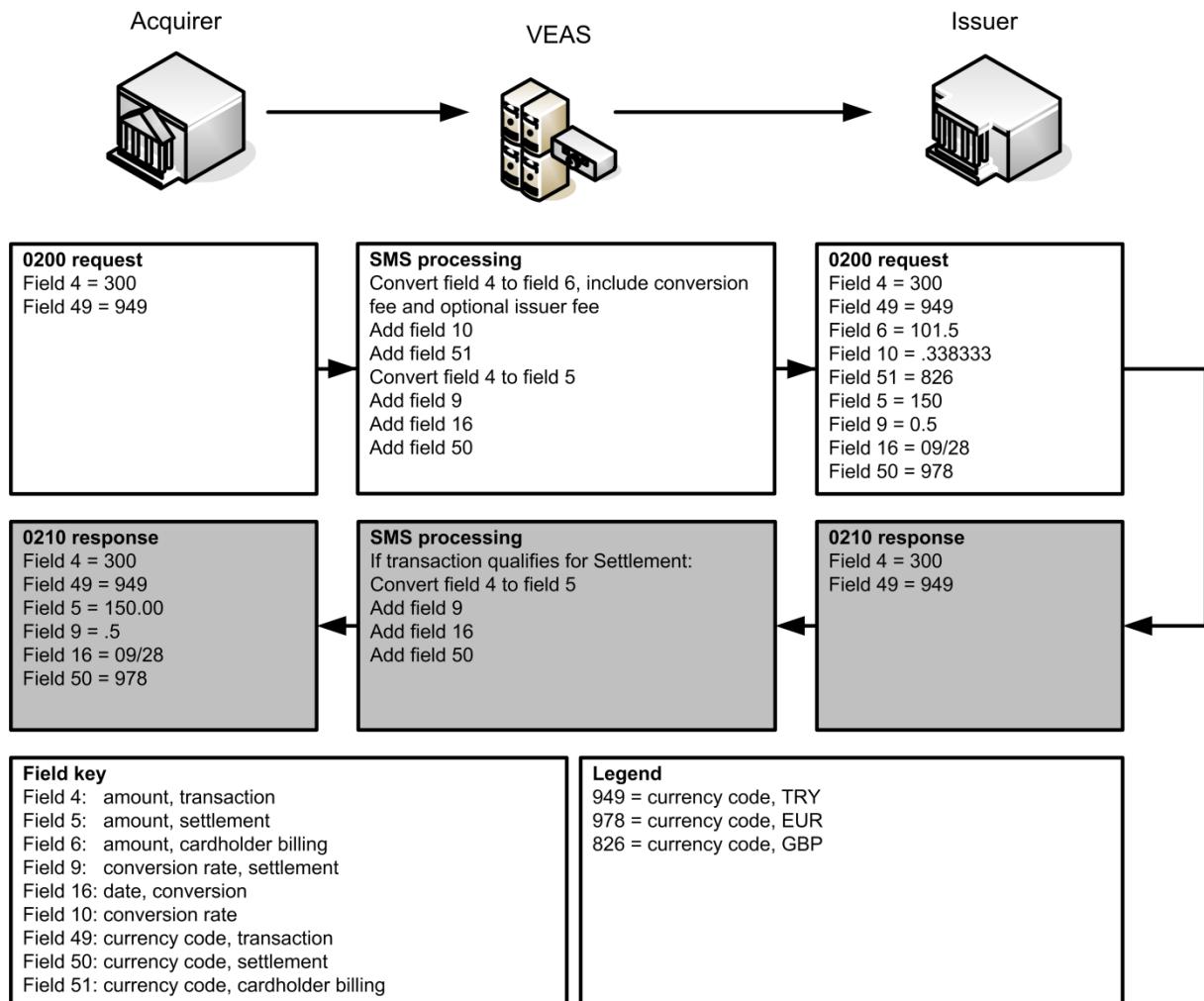
22.12.2 Example 2 - SMS purchase transaction

In the following example:

- Cardholder account is in pounds sterling (GBP)
- Cardholder purchases an item in Turkey (TRY)
- Acquiring bank settles in Euros (EUR)
- Currency conversion rates are:
 - TRY 1 = EUR 0.5
 - GBP 1 = EUR 1.5

- Visa conversion fee plus OIF is GBP 1.5

Figure 50: Multicurrency transaction example 2



1. The Acquirer sends a 0200 request to VEAS.
2. VEAS performs SMS processing and forwards the request to the Issuer.
 - The value in field 10 is calculated by dividing the value in field 6 by that in field 4.
 - The value in field 9 is calculated by dividing the value in field 5 by that in field 4.
3. The Issuer sends a 0210 response.
4. The Acquirer settles in US dollars.

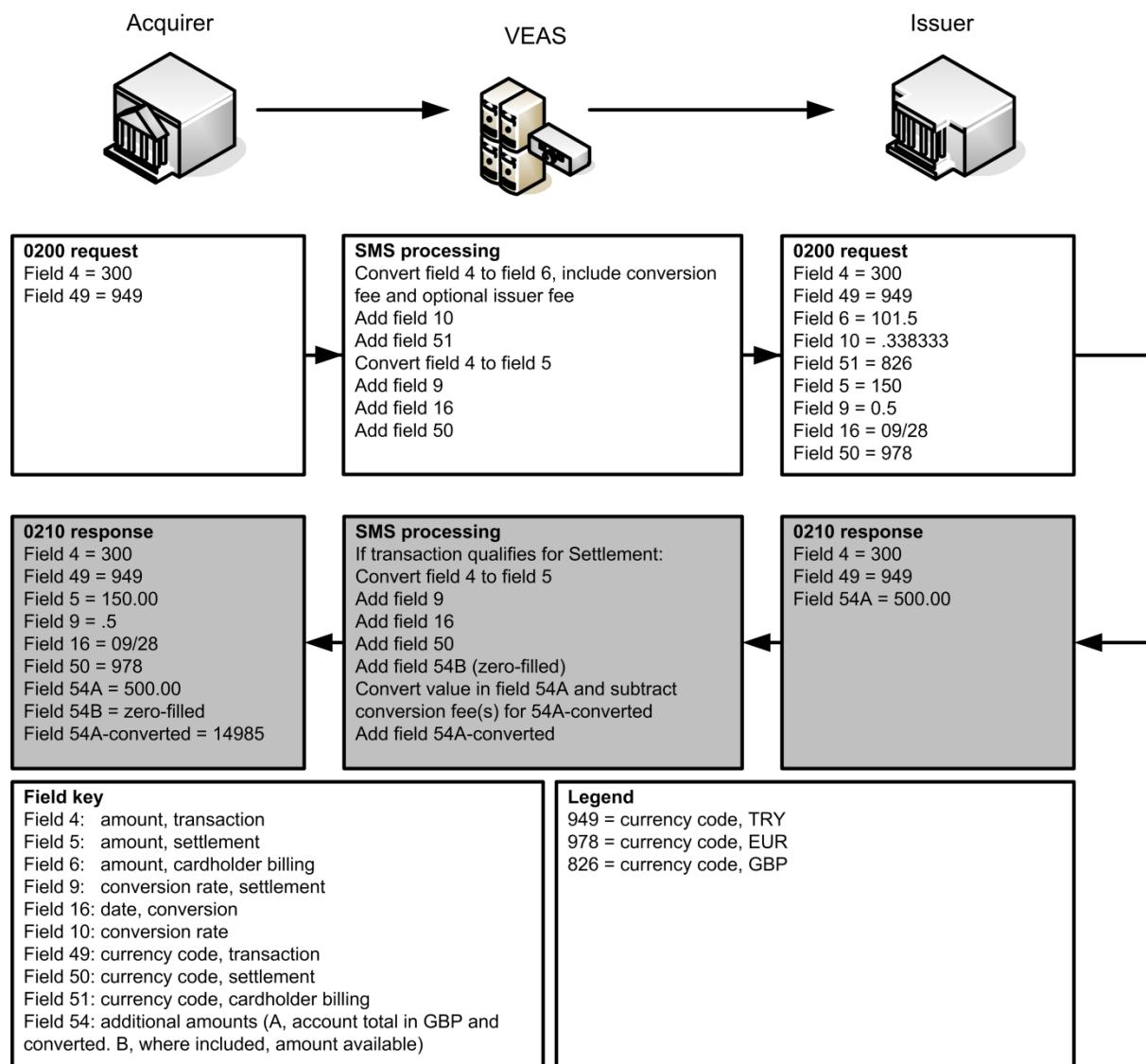
22.12.3 Example 3 - SMS ATM cash withdrawal and balance inquiry

In the following example:

- Cardholder account is in pounds sterling (GBP).
- Cardholder withdraws 300 Turkish Lira (TRY) from an ATM in Turkey and requests an account balance. The enquiry service returns the account balance in both the Cardholder's account currency (GBP) and the equivalent in local currency (TRY).
- Acquiring bank settles in Euros (EUR).

- Currency conversion rates are:
 - TRY 1 = EUR 0.5
 - GBP 1 = EUR 1.5
- Visa conversion fee plus OIF is GBP 1.5.

Figure 51: Multicurrency transaction example 3



1. The Acquirer sends a 0200 request to VEAS.
2. VEAS performs SMS processing and forwards the request to the Issuer.
3. The Issuer sends a 0210 response.

23 National Net Settlement

National Net Settlement (NNSS) is part of the Visa Europe Settlement Service (VSS), which performs settlement for transactions that are cleared through Dual Message System Clearing (DMSC) and the Single Message System (SMS) in a single, centralised service.

Visa Europe has the following national nets:

- Croatia
- Czech Republic
- Hungary
- Iceland
- Poland
- Romania
- Sweden
- United Kingdom

NNSS enables Members located in the same country to settle qualifying Domestic Transactions quickly, through local clearing systems. Qualifying transactions are those for which all the following conditions are met:

- Both Issuer and Acquirer participate in N NSS
- The transaction is a Domestic Transaction
- The Transaction Currency is supported by N NSS

For information on the appropriate setting for the settlement flag, see the *Dual Message System Clearing (DMSC) Technical Specifications*.

23.1 Related information

For further information about VSS, of which N NSS is a part, see the following documents:

- *Visa Europe Settlement Service (VSS) User's Guide*
- *Visa Europe Settlement Funds Transfer Guide*
- *Dual Message System Clearing (DMSC) Technical Specifications*

To arrange implementation of this service, contact Visa Europe Customer Support.

23.2 Participation

N NSS is available through VECSS.

Note SMS is not currently supported by all N NSSs. For information on whether SMS is supported by your N NSS, contact Visa Europe Customer Support.

In countries with an N NSS, it is mandatory for Members to process qualifying transactions through the service.

For more information, see the *Visa Europe Settlement Funds Transfer Guide*.

23.3 How the service works

The main steps in N NSS are:

1. The Visa Europe System collects Interchange Files containing transactions from Members.
2. DMSC and SMS perform clearing and editing on all transactions.
3. After the close of the Settlement Window, the cleared transactions are sent to VSS.
4. VSS processes the settlement records and delivers VSS settlement reports that detail the net Settlement Amount to Members' Visa Extended Access Servers (EA Server) on a daily basis.

Note To view your settlement position, you can use your VSS reports or, if you participate in the UKN NSS (UK National Net Settlement), the SNN NSS (Sweden National Net Settlement), the IS NN NSS (Iceland National Net Settlement) or the HRN NSS (Croatia National Net Settlement), you can use Visa Online to view the Daily Net Settlement Service Positions (DNSSP) page.

5. Funds transfer takes place. During this step, funds are paid from Members in a net issuing position, and paid to Members in a net acquiring position.

23.3.1 Clearing and settlement timing

See the *Visa Europe Settlement Service (VSS) User's Guide* for details about the settlement processing schedule for each National Net Settlement service, including its cut-off time, file delivery time and Settlement Date.

23.3.2 Funds transfer

Funds transfer is the movement of funds due to or from a Member on the N NSS for the purpose of settlement. Funds transfers represent the net position of a Member's credits and debits:

- Members in a net debit (issuing) position pay funds
- Members in a net credit (acquiring) position receive funds

Visa Europe moves funds on working days.

An FTSRE can only have funds transferred to or from a single settlement account. However, if a Member has several FTSREs that belong to different settlement services, each FTSRE can use the same account or use different accounts.

Funds must be settled in the currency supported by N NSS. The times when funds transfer is due depends on the National Net Settlement used, see the *Visa Europe Settlement Service (VSS) User's Guide*.

For more information on the specific settlement processes for National Net Settlement, contact Visa Europe Treasury: [votreasury@visa.com](mailto:vetreasury@visa.com).

For more information about Settlement Currencies and the funds transfer process, see the *Visa Europe Settlement Funds Transfer Guide*.

23.3.2.1 Paying funds to Visa Europe

On some national nets, Members can choose whether funds they owe are paid manually or are collected via automated drawdown of funds. For more information on the options available to you, see the *Visa Europe Settlement Funds Transfer Guide* or contact Visa Europe Treasury.

Funds paid manually are settled as follows:

1. You determine your settlement position from your VSS reports or, if you participate in a national net that enables you to use Visa Online to do this, from the DNSSP page.
2. You create a funds transfer from your Settlement Bank to the settlement agent bank account.

23.3.2.2 Receiving funds from Visa Europe

Visa Europe's designated settlement agent forwards the amount owed to Members that are in a credit position.

24 Partial Authorization

The Partial Authorization service enables Issuers and Processors to part authorize a transaction, where the Cardholder's available balance, or the remaining balance on a Prepaid card, is less than the Transaction Amount requested by the Merchant.

The Partial Authorization service supports multicurrency transactions.

24.1 Related information

For further information about the Partial Authorization service, see the following documents:

- *Dual Message System Authorization (DMSA) Technical Specifications*
- *Single Message System (SMS) POS Technical Specifications*
- *Dual Message System Clearing (DMSC) Technical Specifications*
- *PCI Data Security Standard* (available on the Payment Card Industry, Security Standards Council website)

24.2 Participation

Partial authorization is available through the Visa Europe Authorization Service (VEAS) to users of Dual Message System Authorization (DMSA) and the Single Message System (SMS).

Participation is:

- Mandatory for Acquirers that process AFD transactions
- Mandatory for Issuers

To participate in the service, Members must meet the following requirements.

24.2.1 Issuer implementation considerations

Issuers must be able to support partial authorization reversals.

Issuers of Prepaid cards must be able to support balance return. For more information, see [Prepaid cards](#) on page 201.

For more information on implementing the service, Members should contact Visa Europe Customer Support.

24.2.2 Acquirer implementation considerations

Acquirers participating in the service must be able to send partial authorization transactions and reversals.

Acquirers participating in the service that also process Prepaid cards must be able to support balance return.

Note Such Acquirers do not need to support balance return for AFD transactions.

For more information on balance return, see [Prepaid cards](#) on page 201.

For more information on implementing the service, Members should contact Visa Europe Customer Support.

24.2.3 Testing and certification

Certification is mandatory for participation in the Partial Authorization service.

Visa Member Testing Service (VMTS) provides testing and certification assistance for Members. For more information, Members should contact Visa Europe Customer Support.

24.3 How the service works

The following process describes how a multicurrency partial authorization is progressed for a POS transaction. The principle is the same for a single currency transaction, except that no Currency Conversion Rates are required. In the example, the currency sent in the authorization request is different from the Billing Currency.

1. Merchant forwards a purchase transaction to the Acquirer.
 - Cardholder tenders a card to pay for a purchase
 - The Transaction Amount is in excess of the Cardholder's available balance
2. The Acquirer creates an authorization request and sends it to VEAS.
 - An authorization request is created for the full amount
 - A currency code is always included, even if it is a domestic transaction
 - The message is flagged to indicate that the Merchant can process partial authorizations

Field	Name	Value (bytes)	Description
4	Amount, Transaction	n(12)	Full Transaction Amount, in Transaction Currency
49	Currency Code, Transaction	n(3)	Indicates the field 4 currency
60.10	Additional POS Information, Additional Authorization Indicator	1 or 3	Indicates that the Merchant's terminal can process partial authorizations

3. VEAS forwards the authorization request to the Issuer.
VEAS calculates the Transaction Amount in the Billing Currency and applies any optional Issuer fee (OIF) and conversion fee. Multicurrency fields are added.

Field	Name	Value (bytes)	Description
6	Amount, Cardholder Billing	n(12)	Transaction Amount, in Billing Currency: includes fees
10	Conversion Rate, Cardholder Billing	n(8)	Rate used in calculating field 6
51	Currency Code, Cardholder Billing	n(3)	Indicates the Billing Currency

4. The Issuer edits the message and sends an authorization response to VEAS.

The Issuer checks the Cardholder's available balance. If the balance is less than the Transaction Amount, and the Merchant is a participant in partial authorization, the response message indicates that the authorization is for a partial, and not the full amount.

Field 6 is recalculated as the approved partial amount in the Billing Currency.

Field	Name	Value (bytes)	Description
4	Amount, Transaction	n(12)	Full Transaction Amount, in Transaction Currency
6	Amount, Cardholder Billing	n(12)	Recalculated as approved partial amount in Billing Currency
10	Conversion Rate, Cardholder Billing	n(8)	Rate used in calculating field 6
49	Currency Code, Transaction	n(3)	Indicates the field 4 currency
39	Response Code	10	Indicates that the approval is for a partial amount and not the full amount
51	Currency Code, Cardholder Billing	n(3)	Indicates the field 6 currency
54A	Additional Amounts		First data set [partial authorization]
54A.2	amount type	57	Indicates the use of field 54A.5, which for a partial authorization is 'original amount'
54A.5	amount	n(12)	Original amount; the full Transaction Amount in Transaction Currency

5. VEAS edits the authorization response and forwards it to the Acquirer.

Field 4 is recalculated as the approved partial amount in Transaction Currency.

The approved partial amount in Billing Currency is not forwarded.

Field	Name	Value (bytes)	Description
4	Amount, Transaction	n(12)	Recalculated as approved partial amount, in Transaction Currency

6. The Acquirer routes the authorization response to the Merchant.
7. The Merchant advises the Cardholder and requests additional tender.
 - The Merchant advises the Cardholder of the approved amount, and the balance required to complete the purchase
 - If the Cardholder agrees to continue the purchase, the transaction can complete. The following transaction details are printed on the sales receipt:
 - Approved amount
 - Additional tender amount
 - If the Cardholder does not wish to complete the transaction, the Merchant must immediately initiate a transaction reversal equal to the approved amount
8. The Acquirer submits a clearing transaction for the approved amount.

24.3.1 Reversals

If a transaction is cancelled and that transaction was approved with a partial authorization, the participating Merchant must process a reversal message for the amount of the partial authorization and not the original amount in the authorization request.

24.3.2 Prepaid cards

Members that issue or process Prepaid cards must also support balance return.

Balance return prints the Prepaid card balance on the sales receipt following a successful purchase. This occurs irrespective of whether the transaction was fully authorized or received a partial authorization.

For more information, see the *Visa Europe Prepaid Card Products, Partial Authorization and Balance Return, Member Implementation Guide*.

24.3.2.1 Issuers

Issuers participate in balance return at account range level. Participation is set at one or more account ranges under a specific BIN, depending on the account product range.

Balance return information is forwarded to the Acquirer based on global Balance Return Service processing rules used within VEAS, and the Acquirer's ability to receive field 54 - Additional Amounts, and forward the information to participating Merchants.

24.3.2.2 Acquirers

Acquirers must notify Merchants that they:

- Must print the Prepaid card balance on the sales receipt and give the receipt to the Cardholder
- Must not display the balance amount on the terminal for the Cardholder, or anyone else, to view

Dual message Acquirers must use the amount in field 4 - Amount, Transaction of the Issuer response message, to populate the source amount in the transaction component record TC 05.

24.3.2.3 Stand-in processing

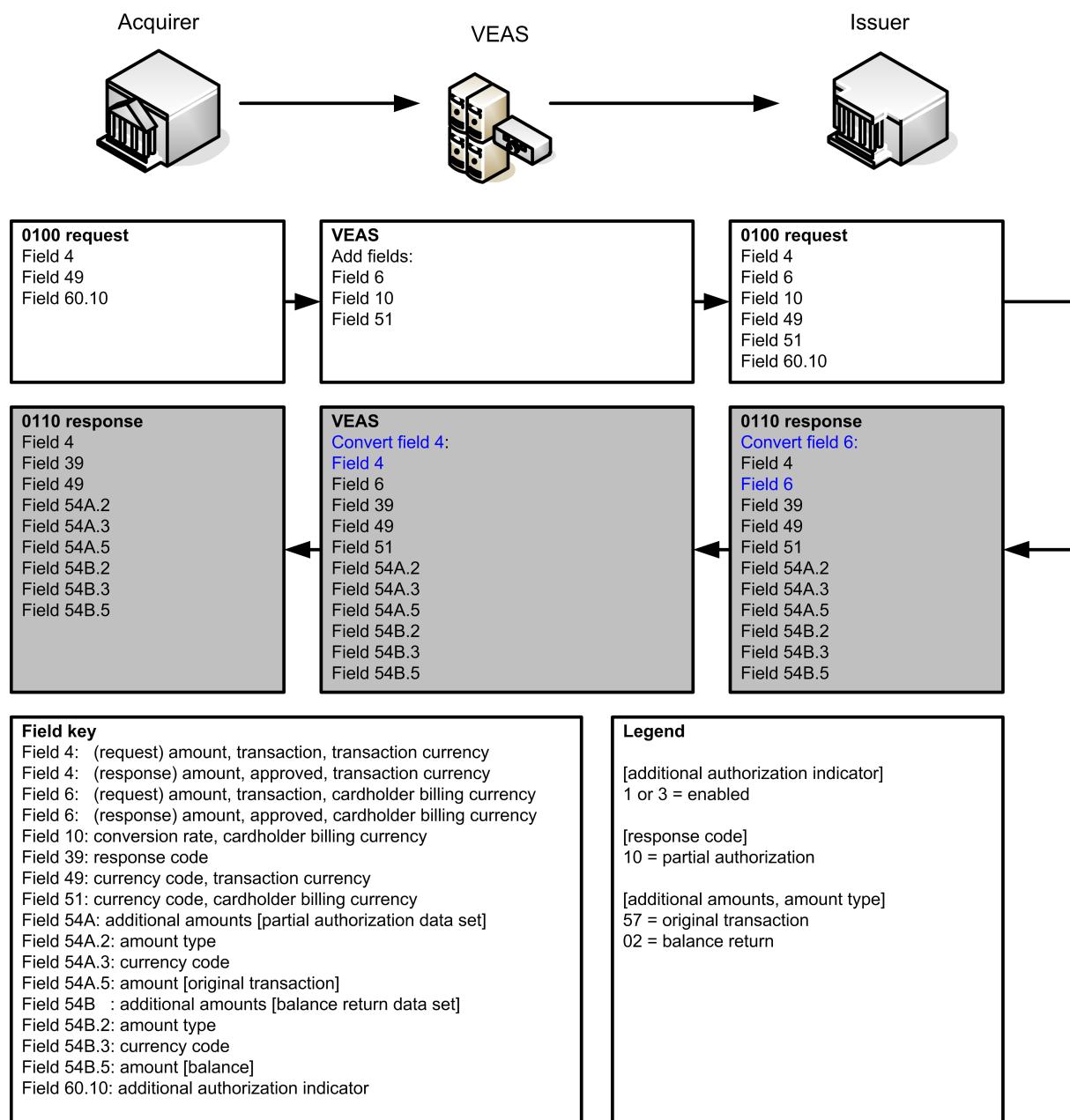
Stand-in processing (STIP) is not available with Prepaid cards; such card transactions will be declined by STIP.

24.3.2.4 Split tender credits

If a Cardholder returns goods purchased as part of a partial authorization transaction, the Merchant must only process the amount paid for by the Prepaid card. The remaining amount must be dealt with according to the Merchant's own returns policy.

24.4 Message flow

The following diagram illustrates the message flow for the Partial Authorization Service.

Figure 52: Message flow for the Partial Authorization Service

24.5 Key messages

The following messages carry the Partial Authorization service:

- 0100 authorization request
- 0110 authorization response
- 0200 financial transaction request
- 0210 financial transaction response

24.6 Key data fields

The following key data fields are used by the Partial Authorization service. For detailed information, see the Visa Europe technical specifications.

Data field 4 - Amount, Transaction

This field contains the Transaction Amount, and is used in both single and multicurrency processing.

Data field 6 - Amount, Cardholder Billing

This field contains the Cardholder billing amount, and is used in multicurrency processing.

Data field 10 - Conversion Rate, Cardholder Billing

This field contains the conversion rate used when calculating amounts in the Billing Currency.

Data field 39 - Response Code

This field contains a value of 10 for a partial authorization transaction.

Data field 49 - Currency Code, Transaction

This field contains a code indicating the Transaction Currency.

Data field 51 - Currency Code, Cardholder Billing

This field contains a code indicating the Billing Currency.

Data field 54 - Additional Amounts

This field contains transaction and balance return information.

Data field 60.10 - Additional POS Information, Additional Authorization Indicator

This field indicates whether a Merchant is able to process a partial authorization. To do so, this field must have a value of '1' or '3'. If it does not, partial authorization cannot take place.

25 PIN Management Service

The PIN Management Service allows Cardholders to change or unblock their PINs at an ATM. A PIN is blocked when the number of failed attempts to enter the correct PIN exceeds the number permitted by the Issuer. The service can be used domestically and internationally by Cardholders of any participating Issuer at ATMs of any participating Acquirer.

Note The PIN Management Service is applicable only to the Visa Smart Debit/Credit (VSDC) card environment. That is, it is restricted to chip-enabled cards and ATMs.

Issuer-to-Acquirer fees apply when the service is used.

25.1 Related information

For further information about the PIN Management Service, see the following documents:

- *Payment Card Industry (PCI): PIN Security Requirements Manual*
- *Visa Europe Merchant Data Standards Manual*

25.2 Participation

The PIN Management Service is available through the dual and single messaging systems. The service is available only at participating ATMs to Cardholders of participating Issuers. Participation is:

- Mandatory for ATM Acquirers in Poland
- Optional for all other Issuers and Acquirers

To participate in the service, Members must meet the following requirements.

25.2.1 Issuer implementation considerations

Issuers must meet the following implementation considerations:

- Issuers must be certified to participate in the service
- Issuers must be certified to send/receive full Visa Smart Debit/Credit (VSDC) data

25.2.2 Acquirer implementation considerations

Acquirers must meet the following implementation considerations:

- Acquirers must be certified to participate in the service
- Acquirers must be certified full Visa Smart Debit/Credit (VSDC) participants

25.2.3 Testing and certification

All participants must be registered and certified. For more information, Members should contact Visa Europe Customer Support.

25.2.4 Service monitoring

There is no monitoring for the PIN Management Service.

25.2.5 Planning and implementation

Participation in the service, for both Acquirers and Issuers, is a Member parameter option maintained by Visa Europe. To participate, Members must complete a *Member Information Questionnaire* detailing their requirements and successfully complete all certification requirements.

For more information, Members should contact Visa Europe Customer Support.

25.3 How the service works

The PIN Management Service enables Cardholders to change or unblock their PIN whilst at an ATM. Acquirers and Issuers must participate in the service and be full VSDC participants.

The following process illustrates how PIN change and unblock requests are progressed:

1. Cardholder requests a PIN change or unblock.
 - Cardholder enters the current PIN followed by the new PIN twice to change it
 - Cardholder interaction for unblocking a PIN is specific to the ATM Acquirer
2. The Acquirer creates an authorization request and sends it to VEAS.
 - The message is flagged to indicate that it is a PIN change or unblock request
 - The request includes a zero transaction amount

Authorization request			
Field	Name	Value	Description
3	Processing Code	70	PIN change/unblock
		72	Unblock
4	Amount, Transaction	0	Zero transaction amount

3. VEAS forwards the authorization request to the Issuer. However, VEAS may respond back to the Acquirer immediately if one of the following conditions applies:
 - If the Issuer is unavailable, STIP returns an 'Issuer unavailable' response to the Acquirer. PIN change and unblock requests cannot be processed by STIP, as STIP does not have access to the relevant account data
 - If the Acquirer does not participate in the service, VEAS sends a 'transaction not allowed at the terminal' response
 - If the Issuer does not participate in the service, VEAS sends a 'transaction not permitted to Cardholder' response

4. The Issuer returns an authorization response to VEAS.
 - If the request is approved, the Issuer sends a 'no reason to decline' response
 - Under certain circumstances (such as 'unsafe PIN'), the request may be declined by the Issuer
 - For a successful change/update, a post-issuance script is included in the authorization response instructing the chip to make the relevant update, for example, for a PIN unblock, the PIN-try counter on the card is reset (sets PIN tries to zero)

Authorization response			
Field	Name	Value	Description
39	Response code	85	No reason to decline

5. VEAS edits the authorization response and forwards it to the Acquirer.
VEAS checks that a script for changing or unblocking the PIN is included in the response, and rejects the message if it is not.
6. The Acquirer routes the response to the ATM.
7. A series of commands takes place between the ATM and the card, and the post-issuance script is applied.
8. The Cardholder's PIN is then successfully changed and/or unblocked and a completion message is displayed at the ATM.

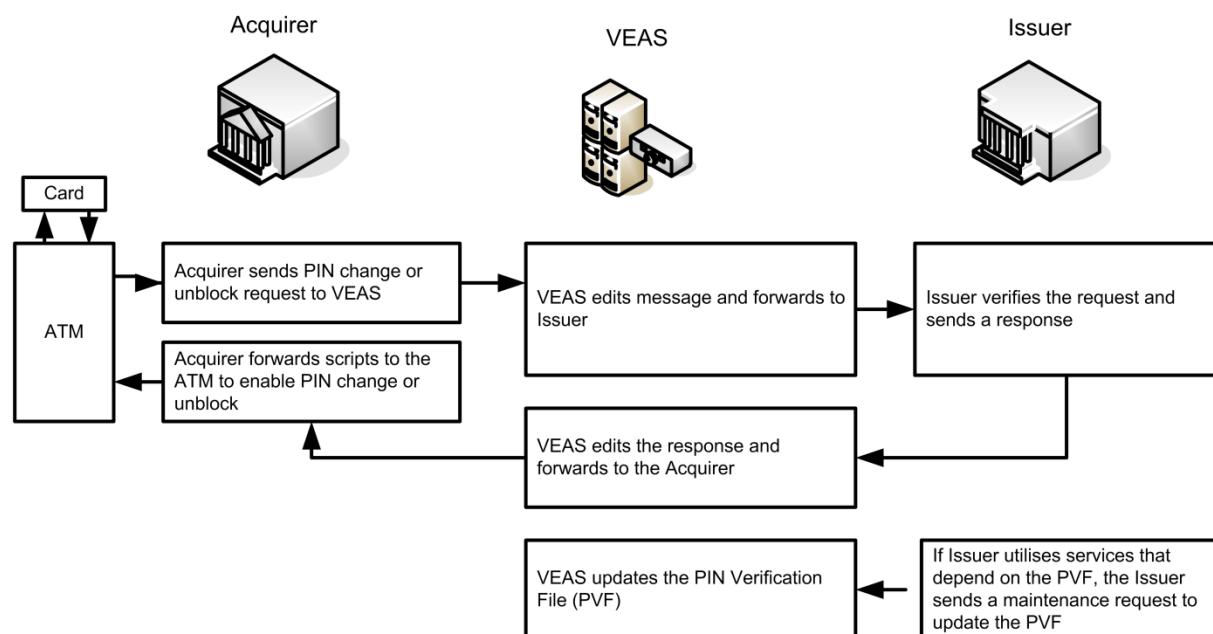
25.3.1 Stand-in processing

Stand-in processing (STIP) is not used. All requests are forwarded to an Issuer. In the event of an Issuer not responding or timing out, VEAS returns a response code of 91 (Issuer not available).

25.4 Process flow

The following diagram illustrates the process flow for the PIN Management Service.

Figure 53: Process flow for the PIN Management Service

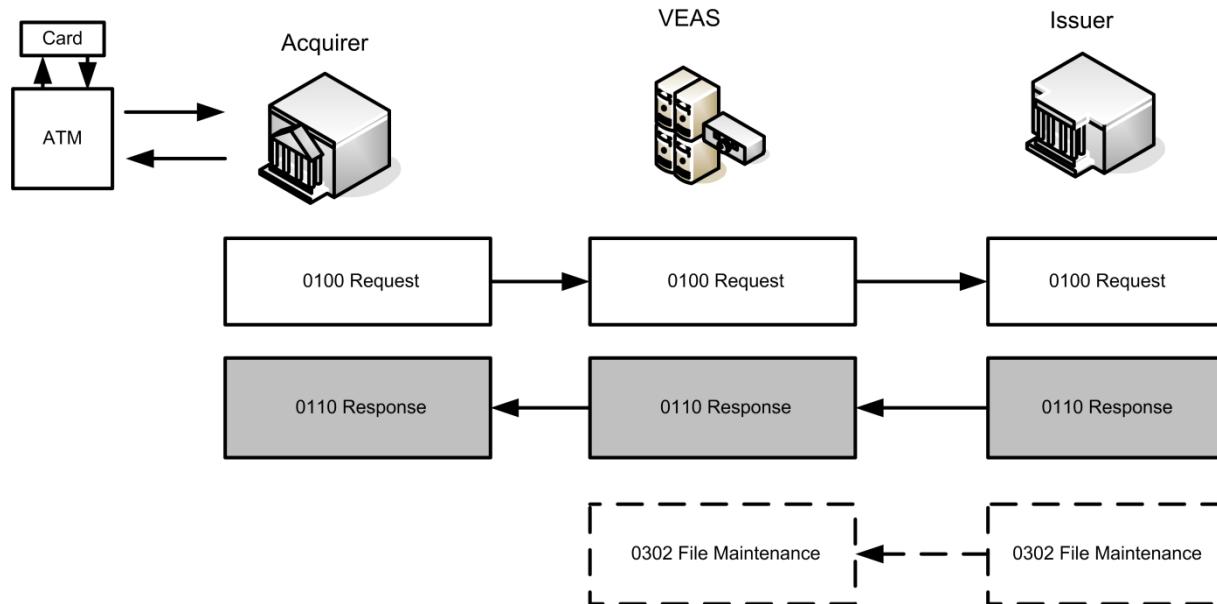


1. Acquirer requests a PIN change or unblock on behalf of the Cardholder.
2. The Issuer responds, approving or declining the request.
3. If approved, the ATM updates the chip card. The card is unblocked, or the PIN changed.
4. If the Issuer is a participant in a service that depends on the PIN Verification File (PVF), the Issuer sends a file maintenance message to VEAS to ensure that the PVF is updated. The PIN held on the Issuer host, on the card itself, and at VEAS in the PVF must be consistent at all times.

25.5 Message flow

The following diagram illustrates the message flow for the PIN Management Service.

Figure 54: Message flow for the PIN Management Service



1. A 0100 authorization request to change or unblock a PIN is sent to the Issuer.
2. The Issuer responds with a 0110 authorization response including a script to change the PIN or to unblock the PIN by resetting the PIN-try counter.
3. If the Issuer participates in a service that depends on the PIN Verification File (PVF), after successful completion of the PIN change or unblock, the Issuer sends a 0302 file maintenance message to update the PVF.

25.6 Key messages

The following messages carry the PIN Management Service:

- 0100 authorization request
- 0110 authorization response

25.7 Key data fields

The following key data fields are used by the PIN Management Service. For detailed information, see the Visa Europe technical specifications.

Data field 2- Primary Account Number

This data field contains the account number of the Cardholder.

Data field 3 - Processing Code

This data field contains a processing code. This must be:

- 70 - PIN change/unblock, or
- 72 - PIN unblock

Data field 18 - Merchant Type

This data field contains the Merchant type, also known as the Merchant Category Code (MCC). This must be set to:

6011 - Financial institutions - automated cash disbursement

Data field 39 - Response Code

This data field contains a code indicating the Issuer's response to the PIN change/unblock request.

Data field 52 - Personal Identification Number (PIN) Data

This data field contains the current PIN, to be replaced by the PIN in field/tag 55/C0 or field 152.

If this field is present, field 53 must also be present.

Data field 53- Security-Related Control Information

This data field contains security data required to process a PIN.

Data field 55 - VSDC Chip Data

This data field contains chip data. Field 55 is mandated for use by all Acquirers.

Data field 142 - Issuer Script

If an Issuer processes the third bitmap, this data field contains the Issuer script command.

Data field 152- Secondary PIN Block

If an Issuer processes the third bitmap, this data field contains the new PIN. The content is encrypted.

26 PIN Routing Service

The PIN Routing Service enables Issuers to route all transactions that require PIN verification to a different Processing Centre from those transactions that do not. The service offers the following options:

- PIN/No-PIN Split Routing option
 - Separates PIN-based transactions from no-PIN transactions and routes them to different Processing Centres.
- POS PIN Routing option
 - Available only to Issuers that use SMS. Routes all POS financial transactions with PINs to an alternative Processing Endpoint.

Each option is separate. Both options cannot be combined.

26.1 Related information

For further information about the PIN Routing Service, see the following documents:

- *Introducing the Visa Europe System*
- *Introducing the Visa Europe Authorization Service*
- *Introducing Single Message System (SMS) and Dual Message System Authorization (DMSA) Transactions*
- *Introducing Single Message System (SMS) and Dual Message System Authorization (DMSA) Messages*
- *Introducing Stand-in Processing*

26.2 Participation

The PIN Routing Service is available through the dual and single messaging systems.

Participation is optional for Issuers and their Processors, subject to the following conditions:

- The PIN/No-PIN Split Routing option supports Visa, V PAY and Visa Electron. The service is also available to non-Visa card issuers such as MasterCard and other card issuing schemes
- The POS PIN Routing option supports SMS only

To participate in the service, Members must meet the following requirements.

26.2.1 Testing and certification

Issuers for both options must be certified for transactions that require PIN verification. Issuers using the POS PIN Routing Service must be certified for SMS processing.

26.2.2 Planning and implementation

To benefit fully from the service and better understand available routing parameters, Issuers should contact Visa Europe Customer Support.

26.3 How the service works

The following sections describe how the service options work.

26.3.1 PIN/No-PIN Split Routing option

VEAS routes incoming PIN and no-PIN requests from Acquirers according to the routing options specified by the Issuer. Issuers can designate one Processing Centre to receive all PIN-based transactions and a different Processing Centre to receive all no-PIN transactions. Issuers can use this option when their own Processing Centres do not have the capability to verify PINs in a secure environment.

Note If a secondary Processing Centre is selected to receive PIN-based transactions, all the parameters associated with that centre will be applied to the transaction. Members must be aware of the Positive Cardholder Authorization Service (PCAS) and stand-in processing (STIP) parameters of both the original and secondary Processing Centres. For more information about STIP and PCAS, see the *Introducing Stand-in Processing* document.

Members that also issue MasterCard cards can use the PIN/No-PIN Split Routing Service to receive their PIN-based and no-PIN MasterCard transactions. That is to say, PIN-based transactions can include cash disbursements if they are destined for BINs belonging to issuers that participate in the Plus program, or if the Member subscribes to the Visa Shortest Online Path (VSOP) Service.

26.3.2 POS PIN Routing option

VEAS routes all POS 0200 financial transactions that require PIN verification to SMS and routes all other transactions to a specified alternative Processing Endpoint. The POS PIN Routing option is available only to Issuers that use SMS to process transactions.

26.4 Process flows

The following sections describe the process flow for the service options.

26.4.1 PIN/No-PIN Split Routing option process flow

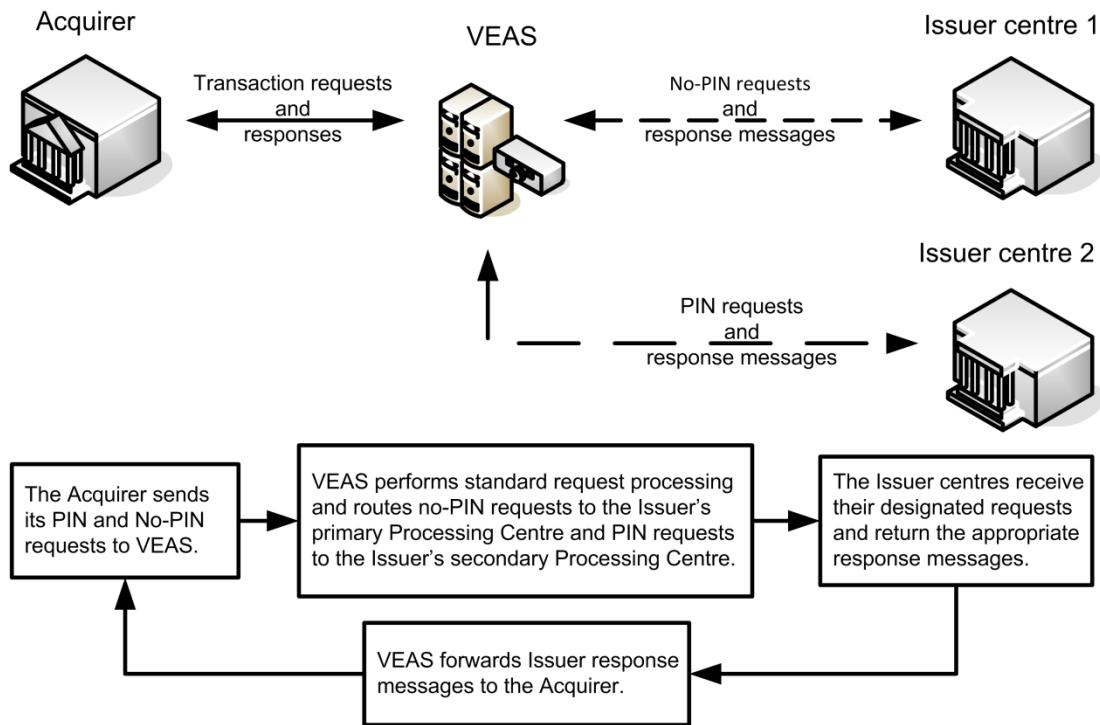
The main steps in the PIN/No-PIN Routing option are:

1. The Acquirer sends requests to VEAS.
2. VEAS routes transactions that require PIN verification to a secondary Processing Centre and routes transactions that do not require PIN verification to the primary Processing Centre.

3. The Issuer's Processing Centres process the requests and return the appropriate responses to VEAS.
4. VEAS forwards the responses to the Acquirer.

The following diagram illustrates the process flow for an Issuer that has designated one Processing Centre for no-PIN transactions (Issuer centre 1) and a different Processing Centre for PIN transactions (Issuer centre 2).

Figure 55: Process flow for PIN/No-PIN Split Routing option

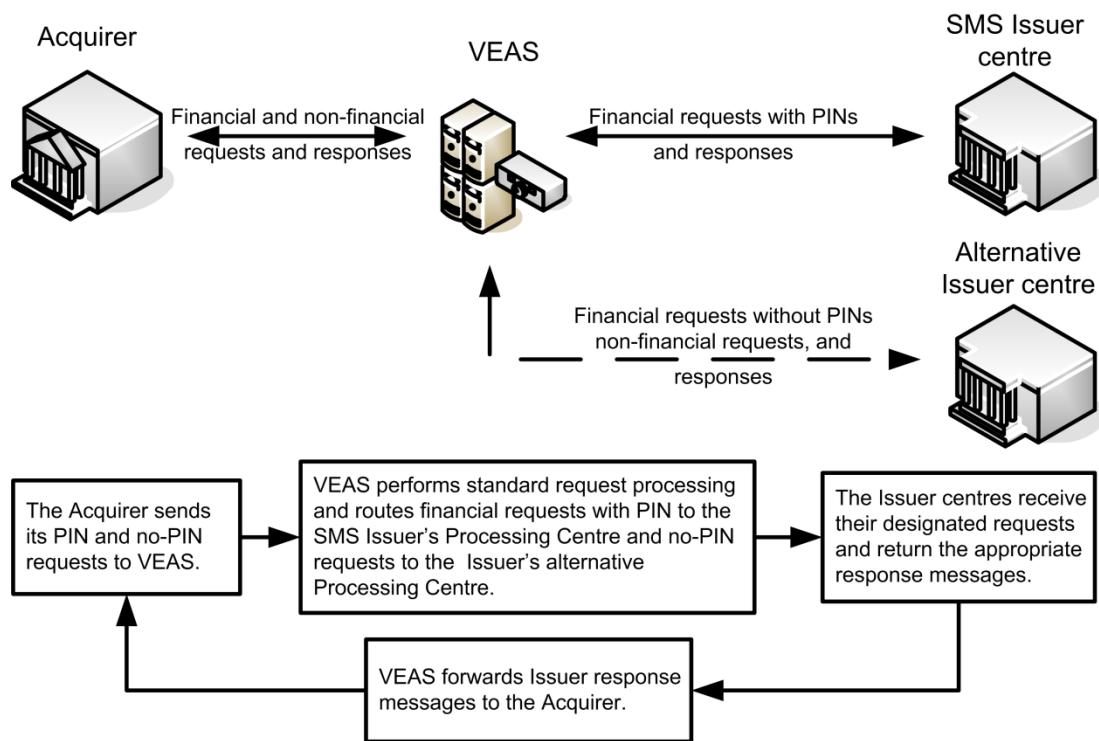


26.4.2 POS PIN Routing option process flow

The main steps in the POS PIN Routing option are:

1. The Acquirer sends transaction requests to VEAS.
2. VEAS routes 0200 financial request messages to the Processing Endpoint for SMS and all other transaction requests to a specified alternative Processing Endpoint.
3. The Issuer's Processing Centres process the requests and return the appropriate response messages to VEAS.
4. VEAS forwards the response messages to the Acquirer.

The following diagram illustrates the process flow for an Issuer that has a designated SMS Processing Centre for POS transaction requests that require PIN verification and an alternative Processing Centre for all other no-PIN transaction requests.

Figure 56: Process flow for POS PIN Routing option

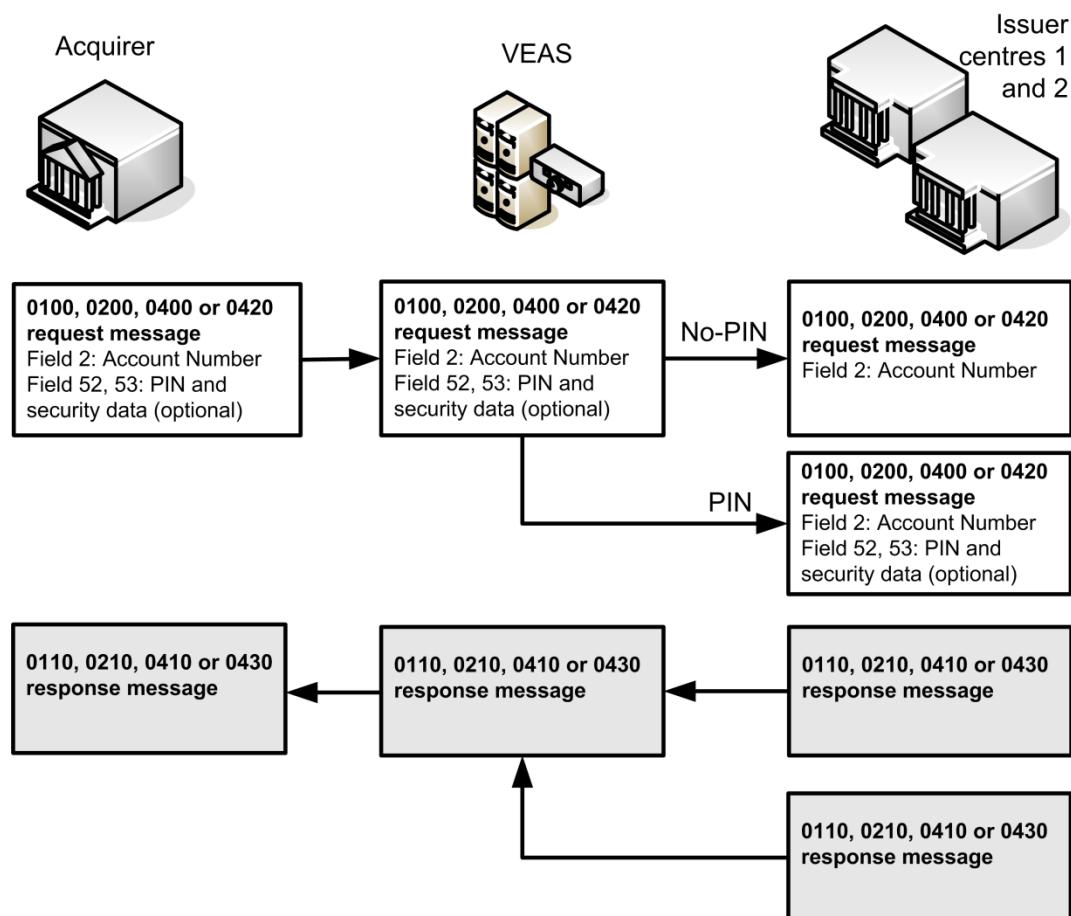
26.5 Message flows

The sections that follow illustrate the message flow for the service options.

26.5.1 PIN/No-PIN Split Routing option message flow

The following diagram illustrates the message flow of the PIN/No-PIN Routing option.

Figure 57: Message flow for PIN/No-PIN Split Routing option

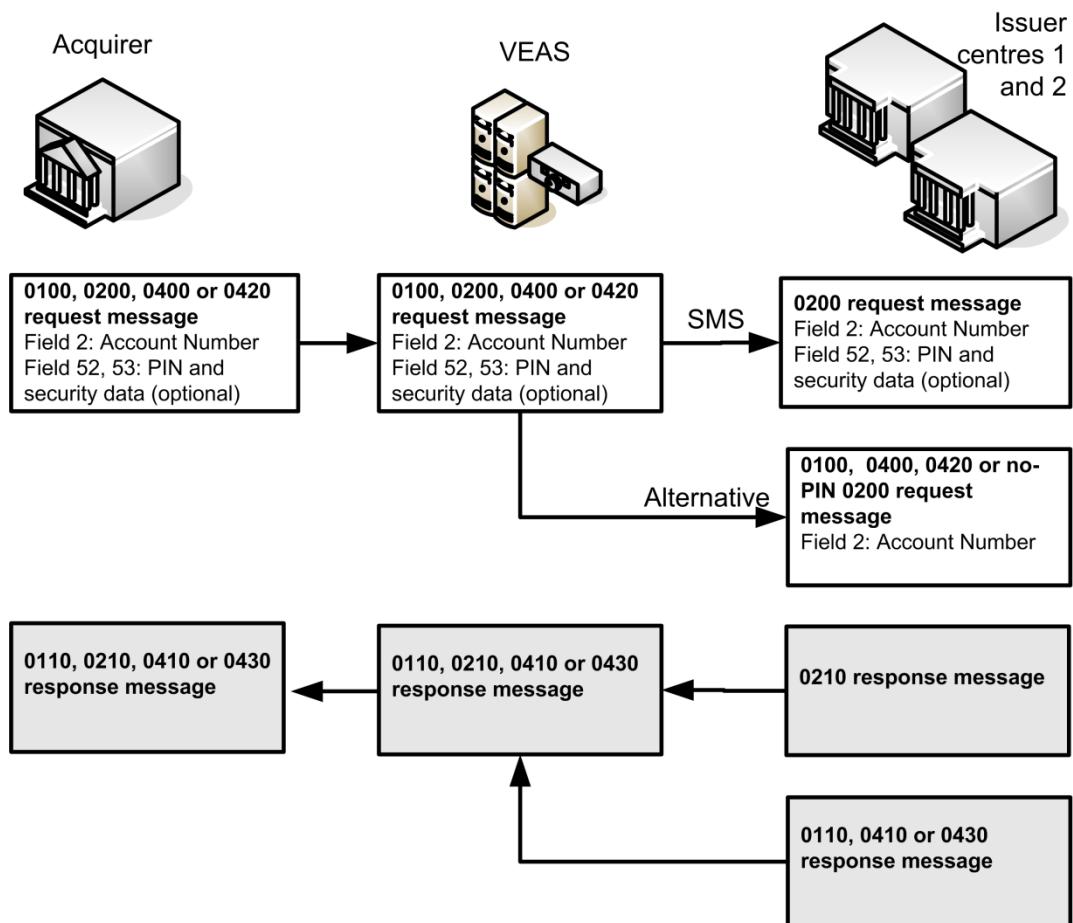


Note Although 0400/0420 reversals carry no PIN data, if they are a reversal of a previous 0100 or 0200 request which did carry PIN data, VEAS routes it to the Processing Centre of the original transaction. This ensures that originals and reversals are processed by the same centre.

26.5.2 POS PIN Routing option message flow

The following diagram illustrates the message flow of the POS PIN Routing option.

Figure 58: Message flow for POS PIN Routing option



Note Although 0400/0420 reversals carry no PIN data, if they are a reversal of a previous 0100 or 0200 request which did carry PIN data, VEAS routes it to the Processing Centre of the original transaction. This ensures that originals and reversals are processed by the same Processing Centre.

26.6 Key data fields

The following key data fields are used by the PIN Routing Service. For detailed information, see the Visa Europe technical specifications.

Data field 2- Primary Account Number (PAN)

This data field contains the account number that is used to determine the routing. The PAN is present in 0100, 0200 and 0400 requests and in 0110, 0210 and 0410 responses.

Data field 52 - Personal Identification Number (PIN) Data

This data field contains the (encrypted) PIN. Data field 52 is used in all requests that require PIN verification. If data field 52 is present, data field 53 - Security-Related Control Information must also be present.

Data field 53 - Security-Related Control Information

This data field contains data needed by the Issuer or the VEAS Security Module to process PINs. This data field must be included in any message that contains a PIN (data field 52).

27 PIN Verification Service

A Personal Identification Number (PIN) is a unique identification code entered by the Cardholder at the Point-of-Transaction to authenticate the identity of the Cardholder and ensure the Cardholder is entitled to make transactions using the card.

There are two forms of verification:

- Online PIN verification
- Offline PIN verification

Important This service description only describes the process of online PIN verification and enables Visa Europe to verify PINs on behalf of the Issuer.

Note The PIN Verification Service (PVS) and the VSDC PIN Management Service are different. The PIN Management Service allows Cardholders to change or unblock their PINs. For more information about this service, see the *PIN Management Service* on page 205.

PVS may be used where the authorization request contains a PIN.

Issuers are responsible for ensuring PINs are verified. PVS offers the following options:

- Full time PIN verification
If an Issuer cannot or does not want to verify its own PINs, PVS can verify all PIN entries on their behalf.
- Stand-in PIN verification
If an Issuer wants to verify its own PINs, when they are not available they can choose to use stand-in processing (STIP) to invoke PVS to verify PINs on their behalf. Visa Europe verifies the PIN and checks the Exception File for special processing requirements. For more information about the Exception File, see the *Visa Europe System Management for Members* document.
- No PIN verification

If an Issuer does not want Visa Europe to verify any PINs.

27.1 Related information

For additional information about the PVS, see the following documents:

- *Introducing the Visa Europe Authorization Service*
- *Dual Message System Authorization (DMSA) Processing Specifications*
- *Single Message System (SMS) ATM Processing Specifications*
- *Single Message System (SMS) POS Processing Specifications*
- *Payment Technology Standards Manual*
- *Visa Europe System Management for Members*
- *Introducing Stand-In Processing (STIP)*

27.2 Participation

PVS is available through the dual and single messaging systems. Participation is optional for Issuers and their Processors.

Important Issuers that issue PINs to Cardholders must provide PIN verification capability themselves and/or subscribe to PVS.

To participate in the service, Members must meet the following requirements.

27.2.1 Issuer requirements

To participate in PVS, Issuers must:

- Select a method for calculating PIN verification Values (PVVs) or offsets
- Provide their PIN Verification Keys (PVKs) to Visa Europe for PIN verification purposes

Each Issuer must use unique PVKs for Visa Europe PIN verification To ensure secure management of the cardholder PIN, the Issuer must use the same key management principles as used for all other cryptographic keys. PVKs must:

- Be unique for each Issuer
- Be unique for each product
- Not be related to any other encryption key except by chance

PIN used in authorization transactions must be processed by hardware security modules (HSMs) in compliance with the PCI PIN Security Standard.

27.2.2 Testing and certification

Certification for PVS is optional.

Certification is recommended if the Issuer is moving from full-time PIN verification service to an in-house PIN processor.

27.2.3 Service monitoring

When an Issuer uses PVS, VEAS monitors transactions that contain PINs and sends the Issuer a warning message when unusual activity occurs. Unusual activity means that one of the following two conditions applies:

- Within a certain period for a given BIN, the number of invalid PIN attempts is unusually high
- For DMSA processing, a large volume of automated transactions has been approved by stand-in processing

In both cases, unusual activity could be the first sign of a security breach or a large-scale attempt to defraud the Issuer.

Important When VEAS discovers unusual activity on an account, it sends the Issuer a warning message. VEAS continues to provide PVS processing on subsequent transactions for that account unless the Issuer sends VEAS a response code to change the status of the account.

27.2.4 Planning and implementation

The following Visa Europe PIN security and encryption rules apply to all authorization transactions:

- PVS participants must use the PVV or IBM PIN Offset verification method
- PINs must be encrypted when they are beyond the protection of TRSMs (Tamper Resistant Security Modules)
- PINs, including encrypted versions, must never be logged
- The Member must use double-length (2 x 8-byte) cryptographic keys (Triple DES)
- Cryptographic keys must be protected during the entire key life cycle, as outlined in the PCI PIN Security Standard
- The Visa Europe key management procedures must be used for Zone Control Master Keys (ZCMKs), Issuer Working Keys (IWKs), Acquirer Working Keys (AWKs) and PVKs

For more information about PIN processing, see the Visa Europe processing specifications. For complete information about PIN processing requirements and standards, see the *Payment Technology Standards Manual*.

To arrange implementation of PVS, contact Visa Europe Customer Support.

27.3 How the service works

PIN verification authenticates the Cardholder. The Issuer or VEAS uses an algorithm to verify the PIN entered by the Cardholder. VEAS utilises the Visa Security Module (VSM), a secure hardware device specifically designed to protect and verify PVVs, to perform PIN verification.

The PVS validates PINs on behalf of Issuers. It also supports MasterCard PIN transactions.

Note VEAS does not send MasterCard PIN-based POS or ATM transactions to MasterCard issuers connected to Banknet. However, VEAS does send MasterCard PIN-based transactions to VEAS or VisaNet-connected Issuers that participate in the PIN/No-PIN Split Routing Service or in the Visa Shortest Online Path (VSOP) Service.

The Visa Europe System currently supports the following methods for calculating encrypted PVVs:

- PVV
- IBM PIN Offset
- Under certain conditions, Issuers can verify their own PVVs using Atalla Technovations encryption systems

Both methods use comparison against a pre-determined verification value - the PVV or the IBM Offset - which is present in the magnetic stripe or held on the Cardholder Database (CDB). Issuers can update the CDB with a replacement verification value if the Cardholder changes their PIN.

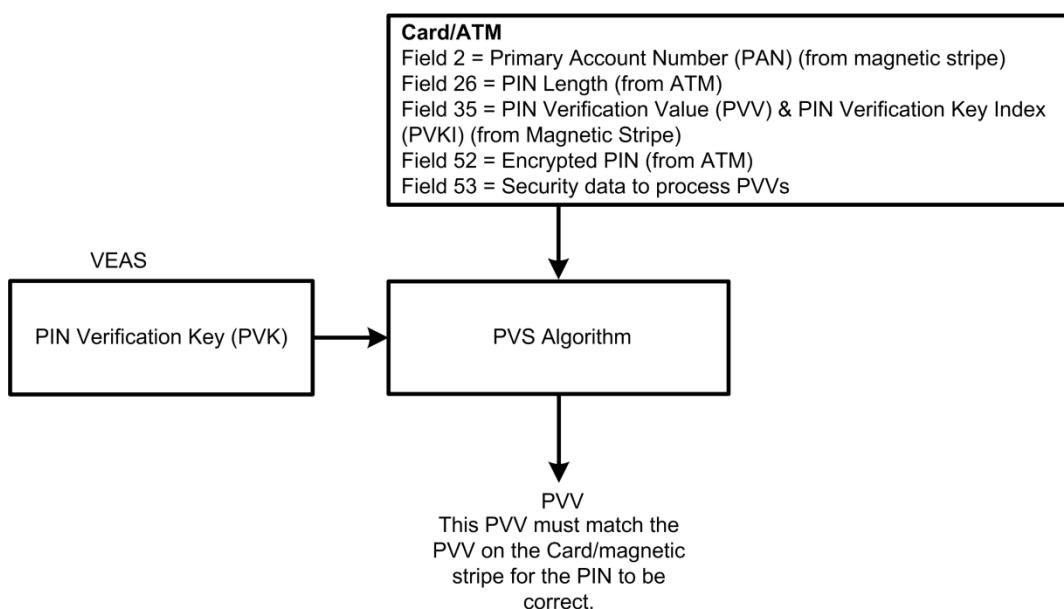
VEAS verifies the PIN and handles the request message based on the authentication results, when:

- A PIN-based authorization or financial request message is received, and
- The Issuer participates in PVS

The main steps in PVS are:

1. The Acquirer sends VEAS a request with an encrypted PIN block.
2. VEAS verifies the PIN using the PVV or IBM PIN Offset verification method. VEAS uses the same Acquirer Working Key (AWK) to decrypt, then uses the PIN, PIN length, received primary account number (PAN) number and the stored PVK to re-create the PVV. It then compares the recreated PVV with the received PVV in the transaction. If these two match, then the PIN is correct.

Figure 59: How the PIN Verification Service works



When verifying the PIN, VEAS first checks the Cardholder Database to determine if the card has a PVV or IBM Offset present. If not in the file, VEAS uses the verification value encoded on the magnetic stripe.

If the PIN is correct, authorization processing proceeds as normal (that is, performing the routing-to-Issuer or stand-in determination). Issuers receiving a request from VEAS can therefore process the transaction in the knowledge that the PIN has been validated as correct.

If the PIN is not correct, or the maximum number of PIN retries has been reached, the authorization is forwarded immediately to STIP. A full set of STIP processes ensues

(such as exception file check). Once complete, and if there is no further problem with the request, then VEAS responds back to the Acquirer with 'invalid PIN'. An advice message is also created for the Issuer.

3. The Issuer receives the request message.

As well as verifying the PIN, the PVS checks to prevent the trial-and-error entry of a PIN.

VEAS records each incorrect PIN entry and accumulates the total in the activity file of the Cardholder Database. For information about the activity file, the PIN Verification File and the Cardholder Database, see the *Visa Europe System Management for Members* document.

The Issuer can set the permitted number of unsuccessful PIN entries for one card. If the limit that is set by the Issuer is exceeded and the correct PIN is finally entered, VEAS still declines the transaction. The PIN retry counter is reset to zero:

- If the correct PIN is entered before the limit of incorrect PIN tries is reached; or
- At 0000 GMT (thus allowing further attempts)

27.3.1 PIN Verification Value method

The PVV method of PIN verification is a mathematical transformation of the account number and PIN performed by a Data Encryption Standard (DES) algorithm.

In addition to the account number and the Cardholder PIN, the algorithm incorporates the following:

- A PIN Verification Key Index (PVKI) value
- A pair of PVK values

The PVKI references one of up to six PVK pairs used in the PVV algorithm.

Note A PVKI value of 0 (zero) indicates that the PIN cannot be verified through PVS.

The Issuer stores the resultant PVV (and its associated one-digit PVKI) on the magnetic stripe of the card and/or in a PIN database with the Processor, or within their systems and/or the PIN Verification File of the Visa Cardholder Database.

To verify a Cardholder's PIN entry, the Issuer or VEAS uses the following to calculate a transaction PVV:

- The PIN entered at the terminal by the Cardholder
- A portion of the PAN
- The PVKI
- VEAS BIN data: magnetic stripe PVKI/PVV location, PVK

VEAS uses a validation process on a physically secure, dedicated hardware security module to compare the reference PVV to the transaction PVV. To successfully validate the PIN and the Cardholder, the transaction PVV and the reference PVV must match.

27.3.2 IBM PIN offset method

The IBM PIN Offset verification method of PIN verification is a mathematical transformation of the account number and PIN performed by a DES algorithm.

In addition to the account number and the Cardholder PIN, the algorithm incorporates the following:

- An IBM PVK (IBMKEY)

The Issuer stores the resultant PIN Offset value on the magnetic stripe of the card, and/or in a PIN database with the Processor or within their systems, and/or the PIN Verification File of the Visa Cardholder Database.

To verify a Cardholder's PIN entry, the Issuer or VEAS uses the following to calculate a transaction PVV:

- The encrypted PIN entered at the terminal by the Cardholder
- A portion of the PAN
- The reference PIN offset
- VEAS BIN data: decimalisation table, length of offset, displacement in PAN, number of offset characters, pad character, magnetic stripe offset location, IBMKEY

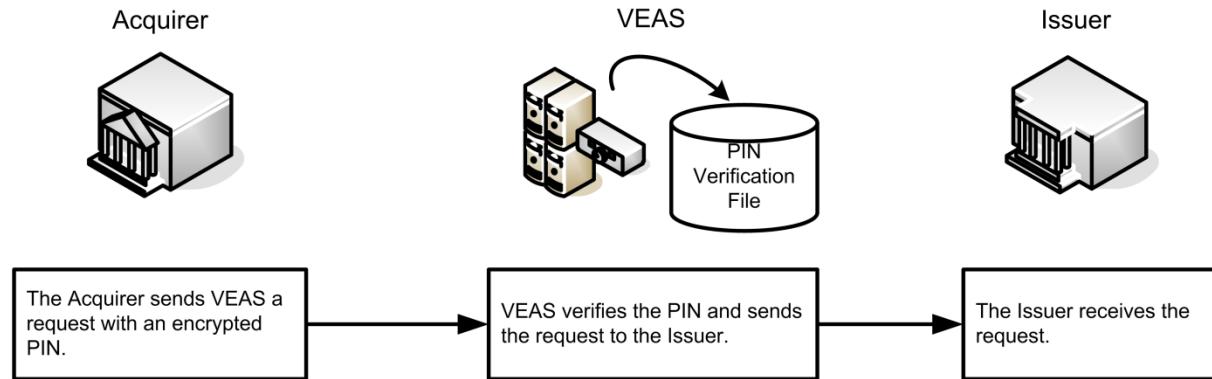
VEAS uses a validation process utilising a physically secure, dedicated hardware security module, to recalculate the PIN based on the PAN and the reference PIN Offset. Within the security module, the recalculated PIN is then compared to the clear PIN decrypted from the authorization request. To successfully validate the PIN and the Cardholder, both calculated PIN and clear PIN must match.

For more information about the IBM PIN Offset method, see the *IBM 3624 Consumer Transaction Facility Programmer's Reference and Component Descriptions* manual. Contact IBM for a copy of this manual.

27.4 Process flow

The following diagram illustrates the process flow of a PIN-based message which utilises the PVS.

Figure 60: Process flow for the PIN Verification Service



The process flow for the PVS is:

1. The Acquirer sends a request with an encrypted PIN to VEAS.
2. VEAS verifies the PIN using the PVV or IBM PIN Offset verification method and sends the request message to the Issuer.
3. The Issuer receives the request message and returns an authorization response.

Authorization messages containing PINs are never sent unencrypted. At each stage, the PIN data is encrypted under a working key: from the Acquirer to Visa under the AWK; from VEAS to the Issuer under the IWK. For more information about PIN translation, see the *Introducing the Visa Europe Authorization Service* document. The working keys must be shared between the Member and VEAS:

- VEAS generates a master key to securely transport the working keys (AWKs or IWKs) to/from the Members.
- The Issuer or the Acquirer may generate their own keys, or have Visa generate a set for them.
- When stored within the VEAS system, all keys are stored as cryptograms. Keys are only decrypted within the confines of the VSM.

When using PVS, VEAS decrypts and verifies the PIN. If the PIN is checked and is valid then processing continues as normal. If the PIN is invalid, STIP is invoked and an advice is generated.

When initiating a PIN check, PVS checks the number of prior unsuccessful PIN-entry attempts to ensure that the limit is not exceeded. PVS maintains a count of consecutive unsuccessful PIN-entry attempts made on the current day for a given account number.

PVS processing is regulated based on the current count of unsuccessful PIN-entry attempts:

- If the count of invalid PIN-entry attempts is already equal to the invalid PIN limit, then PVS automatically assigns the request with a response code of '75' - PIN Entry Tries

Exceeded. The request then goes to STIP as described below.

- When a count exceeds the limit, STIP continues to assign response code 75 to all subsequent requests for the rest of the day. The Cardholder is not able to complete any further transactions that require an online PIN for the rest of the day. The Cardholder can retry the next day after PVS clears the PIN counts at the end of the current day.
- If the PIN is checked and found to be invalid, PVS increases the count by one.
 - PVS then compares the updated count to the limit. If the updated count now exceeds the limit, PVS updates the count and assigns the interim Response Code 75 - Allowable Number of PIN Entry Tries Exceeded to the request message. If the number of invalid PINs is not yet exceeded, then an interim Response Code of 55 - Invalid PIN is assigned.
 - PVS then passes the request to STIP to undergo further checks.
 - STIP then performs a number of additional checks, including:
 - Performing a look-up on the Exception File for a negative code
 - Determining the default response code
 - If STIP does not find a negative code with a greater priority than either '75' or '55', then a response is generated back to the Acquirer.
 - Before responding, if the interim response code is '75', STIP converts this to a '05' decline in the response to the Acquirer.
 - An advice message is created with '55' or '75' for the Issuer.
- If the PIN is checked and found to be valid, PVS clears the count to zero. Normal processing then continues (that is, route to Issuer or to stand-in processing based on transaction risk factors).

To control PIN-retry activity, the Issuer selects the limit for the number of consecutive unsuccessful PIN-entries attempts allowed in a day.

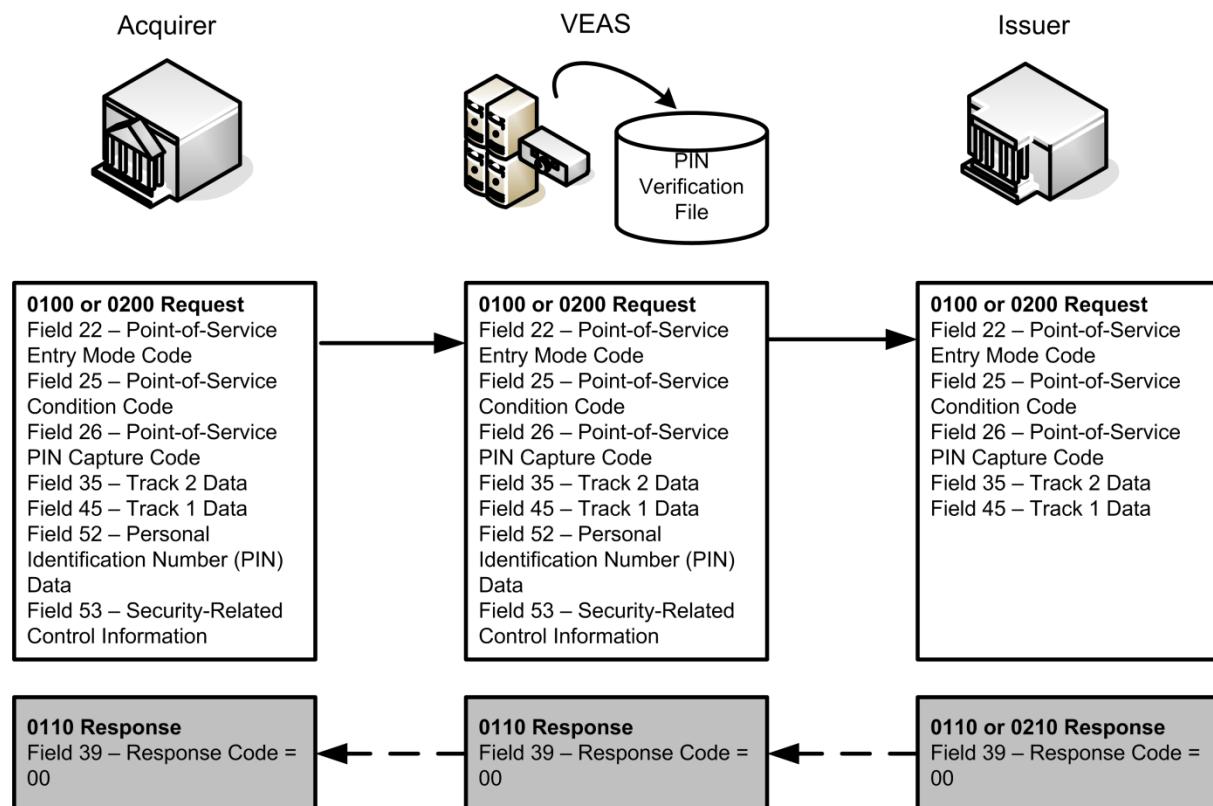
Important VEAS declines the transaction but does not request card pick-up. However, some Members have reciprocal agreements to pick up the cards after the specified number of unsuccessful PIN-entry attempts have occurred.

27.5 Message flow

The following diagrams illustrate the message flows for the PVS, where VEAS always validates the PIN.

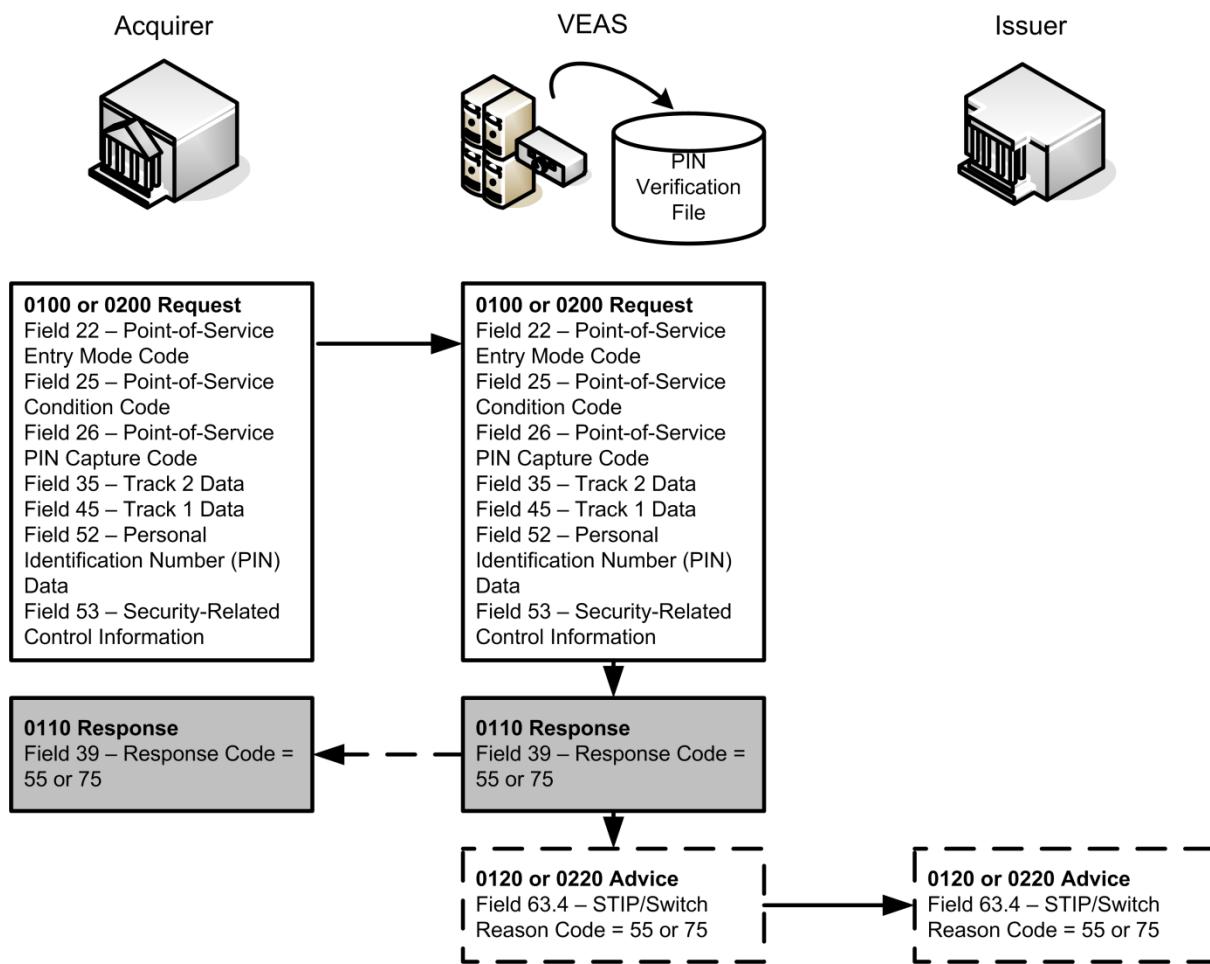
If the PIN is valid, the 0100/0200 request goes to the Issuer and no advice messages are generated.

Figure 61: Message flow for the PIN Verification Service when PIN is valid



If the PIN is declined because it is invalid or the number of invalid PINs is exceeded then the 0100/0200 request goes to STIP and generates an advice message.

Figure 62: Message flow for the PIN Verification Service when PIN is declined



27.6 Key messages

The following messages carry the PIN:

- 0100 authorization request or balance inquiry
- 0120 Advice message
- 0200 Purchase transaction or ATM cash disbursement request
- 0220 Advice message

Note The verification, activity and exception files reside in the Cardholder Database. For information about the database and its files, see the *Visa Europe System Management for Members* document.

27.7 Key data fields

The following key data fields are used by the PVS. For detailed information, see the Visa Europe technical specifications.

Data field 22 - Point-of-Service Entry Mode Code

This data field contains a series of codes that identify the following information about transactions processed by the Visa Europe System:

- When a terminal is used
- The method used to capture the account number and the expiry date
- The PIN capture capability of the terminal

Data field 25 - Point-of-Service Condition Code

This data field contains a value that indicates the transaction conditions at the POS and identifies the type of original or subsequent transaction.

This data field is used in all Cardholder transaction-related 01xx, 02xx and 04xx messages. The code in the original request message is shown in all subsequent messages.

Data field 26 - Point-of-Service PIN Capture Code

This data field contains a value indicating the maximum number of PIN characters accepted by the POS device. It is required when the Acquirer does not support the maximum PIN length of 12 digits. If the Acquirer supports 12 digits, inclusion of the data field is optional.

Data field 32 - Acquiring Institution Identification Code

This data field contains the Acquirer Institution Identification Code that is associated with the AWK used to encrypt the PIN. It is also the identification code for Visa Europe to locate the transport key (AWK for example) if data field 33 does not exist.

Data field 35 - Track 2 Data

This data field contains the location of the PVV. Only Issuers that require the PVV service need to encode PVV on the track data. In addition, Visa Gold cards or above are required to have the PVV position reserved (but it is not necessary to encode the correct PVV). The discretionary data field must contain both the PVV and the CVV.

For more information about format specifications for Track 2, see the *Payment Technology Standards Manual*.

Data field 39 - Response Code

This data field contains a code that defines the response to a request or the message disposition.

This data field is present in all responses except those for reconciliation and most network management functions.

Data field 45 - Track 1 Data

This data field contains the PIN data encrypted on Track 1 of the magnetic stripe. If both Track 1 and Track 2 are present in a message, Track 1 takes precedence.

For more information about the format specifications for Track 1, see the *Payment Technology Standards Manual*.

Data field 52 - Personal Identification Number (PIN) Data

This data field contains a PIN or password, encrypted and formatted as a block of 16 hexadecimal digits.

Data field 53 - Security-Related Control Information

This data field contains data needed by the Issuer or the VSM to process PVVs entered at point of service.

This data field is required in any message containing a PIN in data field 52.

Data field 60 - Additional POS Information

This data field describes the capability of the terminal used. Position 2 relates to the coding in data field 22.

Subfield 63.4 - STIP/Switch Reason Code

This subfield contains a code that identifies why Visa Europe stood in for the Issuer or why VEAS generated an advice message. This subfield is present in an advice message that is generated by STIP when Visa Europe has authorized on behalf of the Issuer.

28 Positive Cardholder Authorization Service

The Positive Cardholder Authorization Service (PCAS) provides a set of risk control services that allow an Issuer to specify transaction processing controls for authorization requests.

These controls:

- Vary according to Merchant type and Cardholder risk level
- Determine which transactions to forward to the Issuer
- Determine the authorization services provided to the Issuer

Issuers establish parameters such as Issuer, advice and activity limits that determine when to route transactions to the Issuer or to stand-in processing (STIP).

If a transaction is routed to the Issuer, the Issuer provides the response. If a transaction is routed to STIP, PCAS processing limits and STIP authorization options determine the response.

PCAS provides options to Issuers to control risk, Cardholder service, and authorization volume and expense by:

- Routing higher-risk transactions to the Issuer
- Processing low-risk transactions in STIP
- Providing stand-in processing during Issuer unavailable conditions

28.1 Related information

For further information about the Positive Cardholder Authorization Service (PCAS), see the following documents:

- *Introducing Stand-In Processing (STIP)*
- *Dual Message System Authorization (DMSA) Processing Specifications*
- *Visa Europe Merchant Data Standards Manual*

28.2 Participation

The Positive Cardholder Authorization Service (PCAS) is available through the dual messaging systems.

Participation is mandatory for Issuers and Processors.

To participate in the service, Members must meet the following requirements.

28.2.1 Issuer and activity limits

The following limits must be established:

- **Issuer limits** for single-Transaction Amounts for each of the 11 standard Merchant category groups (MCGs)

If a transaction is equal to or greater than the Issuer limit, it will be routed to the Issuer for authorization. If the Transaction Amount is below the Issuer limit, the transaction will be routed to STIP for authorization.

To route all transactions to the Issuer, Issuer limits can be set to zero.

See [Issuer limits](#) on page 233.

- **Activity limits** for Total Purchase and Total Cash. Optional activity limits can be established for a further 7 MCGs

Count and amount limits for Issuer available and unavailable conditions. If either limit is exceeded, then depending on Issuer availability, and other processing checks, a transaction may be forward-referred to the Issuer.

Activity limits can be set to zero, to route all transactions to the Issuer.

See [Activity limits](#) on page 235.

In addition to the limits and processing factors mandated for PCAS, Issuers can also specify Cardholder risk levels and random selection parameters.

Note All limits are defined in US dollars (USD); with the exception of limits for Issuers of V PAY, which are in euros.

28.2.2 Service monitoring

Service monitoring is not available for the Positive Cardholder Authorization Service.

28.2.3 Planning and implementation

Members communicate initial PCAS parameters, and any subsequent maintenance requests, to Visa Europe by completing a *Member Information Questionnaire*. For more information, Members must contact Visa Europe Customer Support.

28.3 How the service works

Positive Cardholder Authorization Service (PCAS) provides Issuer control of routing and stand-in processing (STIP). Control is effected through a number of Visa Europe-maintained PCAS parameters.

28.3.1 Routing

Parameters determine when authorization requests should be forwarded to the Issuer or to stand-in processing.

28.3.2 Stand-in processing

A set of parameters for when an Issuer is available, and a complementary set of parameters for when an Issuer is unavailable, determine the appropriate authorization request response:

- Approve
- Decline

- Forward-refer

In certain Issuer available situations where an approval response or a decline response is not appropriate, it is possible to forward-refer the request to the Issuer. If the Issuer is available, the following transactions are always forward-referred.

[Issuer option] indicates that the action is dependent on the Issuer setting this condition:

- Account verifications/address verifications
- PIN verifications processed by the Issuer
- Accounts listed on the Exception File as XA (forward to Issuer, or approve) and XD (forward to Issuer, or decline)
- Balance inquiry [Issuer option]
- Key-entry [Issuer option]
- International [Issuer option]
- Transaction acquired in a 'risky' country [Issuer option]
- Transaction is mail order [Issuer option]

In addition, certain STIP conditions such as activity limits being exceeded can also cause a request to be forward-referred.

28.3.3 PCAS parameters

The majority of PCAS parameters are defined at BIN level, with certain others available at account level. Visa Europe maintains PCAS parameters on behalf of Issuers. Issuers define their requirements and forward them to Visa Europe by completing a *Member Information Questionnaire*.

PCAS parameters are set using the following framework:

- Merchant category groups
- Issuer limits
- Advice limits
- Activity limits
- Mandated minimum limits
- Activity checking
- Cardholder risk levels and individual limits
- Random selection factors
- BIN blocking, country restrictions, risky countries , and country-to-country embargos
- Suppress inquiry (SI) mode

In addition to the transaction type, Merchant category group, geographical jurisdiction, and Issuer processor availability, PCAS utilises Issuer limits to route transactions to the Issuer or to STIP.

Important VEAS sends all risky transactions (for example, e-commerce transactions and online gambling transactions) to the Issuer. If the Issuer is unavailable, STIP processes them according to Issuer-defined parameters.

28.3.4 Merchant category groups

Table 32: Merchant category groups

No.	Merchant category group	Transaction type	Transaction category
1	Commercial Travel	Travel & Entertainment (T&E)	Total Purchases
2	Lodging		
3	Auto Rental		
4	Restaurant		
5	MOTO	Purchases (non T&E)	
6	Risky Purchase		
7	Other Purchase		
11	Medical		
8	Other Cash	Cash	Total Cash
9	ATM Cash		
10	Quasi-Cash		
MOTO is an acronym for Mail Order/Telephone Order. Electronic commerce Merchants are included in this category.			

Merchant category groups (MCGs) are collections of similar Merchant types. Visa has defined 11 MCGs. These categories allow Issuers to apply processing parameters according to common risk and customer service implications.

Each MCG has its own set of related Merchant Category Codes (MCCs). Acquirers assign MCC codes to Merchants; the codes designate a Merchant's principal trade, profession or line of business. For a full listing of MCCs, see the *Visa Europe Merchant Data Standards Manual*.

The 11 MCGs comprise three transaction types: purchases relating to Travel & Entertainment, purchases other than travel & entertainment, and Cash. These types form two transaction categories: Total Purchases, and Total Cash.

28.3.5 Issuer limits

An Issuer limit is a Transaction Amount threshold that determines whether VEAS should route a transaction to STIP or to the Issuer. An Issuer limit is a mandatory requirement for each MCG. An Issuer limit can be set to zero, to ensure that all transactions are forwarded to the Issuer:

- Transactions for amounts equal to or greater than the Issuer limit are forwarded to Issuers for processing
- Transactions for amounts less than the Issuer limit are routed to STIP for processing

When the Issuer is unavailable, STIP can process transactions in accordance with the Issuer unavailable parameters set up for the BIN. In addition to Issuer-defined limits, Visa Europe also imposes a number of mandated minimum limits on International Transactions. These vary, based on card type, and for particular MCGs.

Table 33: Issuer limits

No.	Merchant category group	Issuer limit
1	Commercial Travel	Required
2	Lodging	Required
3	Auto Rental	Required
4	Restaurant	Required
5	MOTO	Required
6	Risky Purchase	Required
7	Other Purchase	Required
11	Medical	Required
8	Other Cash	Required
9	ATM Cash	Required
10	Quasi-Cash	Required

28.3.6 Advice limits

Table 34: Advice limits

No.	Merchant category group	Advice limit
1	Commercial Travel	BIN default
2	Lodging	BIN default
3	Auto Rental	BIN default
4	Restaurant	BIN default
5	MOTO	Zero
6	Risky Purchase	BIN default
7	Other Purchase	BIN default
11	Medical	BIN default
8	Other Cash	Zero
9	ATM Cash	Zero
10	Quasi-Cash	Zero

The advice limit is a Transaction Amount threshold that impacts on below Issuer limit transactions processed by STIP. It determines which STIP processed transactions will generate advice messages and be included in transaction activity checking.

Issuers can specify only one advice limit per BIN. However, irrespective of any Issuer-defined limit, the mandated advice limit for all Cash MCGs and the MOTO MCG is zero.

Additional considerations for STIP processing comprise:

1. Exception File checking
2. Generate Issuer advice message for declined transaction
3. Generate Issuer advice message for approved transaction
4. Include transaction in activity checking

Exception File checking identifies invalid, possibly fraudulent, cards. An advice message is a record of stand-in processing actions undertaken on the Issuer's behalf.

- Transaction Amount below the advice limit
 - Exception File check
 - Advice message generated for a decline response
- Transaction Amount between the advice limit and Issuer limit
 - Exception File check
 - Advice message generated for a decline response
 - Activity check
 - Optional, advice message for an approval response
- Transaction Amount above Issuer limit
 - Exception File check (only checked in STIP. If the transaction is routed to the Issuer and the Issuer is available, then the Exception File is not checked)
 - Advice message generated for a decline response
 - Activity check (the activity check is not actioned if the transaction is routed to, and processed by, the Issuer)
 - Advice generated for an approval response

An advice limit can be equal to, or less than, any MCG Issuer limit. If an advice limit is greater than an Issuer limit, the Issuer limit takes precedence.

The same advice limit applies to both Issuer available and Issuer unavailable conditions.

28.3.7 Activity limits

Table 35: Cardholder activity limits

No.	Merchant category group	1-day activity limit Count	1-day activity limit Amount	4-day activity limit Multiplier
1	Commercial Travel	Optional	Optional	Optional
2	Lodging	Optional	Optional	Optional
3	Auto Rental	Optional	Optional	Optional
4	Restaurant	Optional	Optional	Optional
5	MOTO	Optional	Optional	Optional
6	Risky Purchase	Optional	Optional	Optional

Table 35: Cardholder activity limits (continued)

No.	Merchant category group	1-day activity limit Count	1-day activity limit Amount	4-day activity limi Multiplier
	Total Purchase	Required	Required	Required
9	ATM Cash	Optional	Optional	Optional
	Total Cash	Required	Required	Required

Activity limits enable Issuers to control accumulated Cardholder spending. Activity limits are not available for all Merchant category groups (MCGs). Where an MCG specific limit is not available, the appropriate Total Purchase or Total Cash limit is used.

Activity can be limited through three measures:

- **1-day count**, limiting the number of approved account transactions that can be made in a day
The limit applies to the current day's transactions, and can be set to any integer value between 0 and 250.
- **1-day amount**, limiting the value of approved account transactions that can be made in a day
This limit applies to the current day's transactions, and can be set to any amount between USD 0.00 and USD 65,500.00.
- **4-day count and amount**, limiting the number and value of approved transactions accumulated over a 4-day period

One 4-day multiplier can be applied to a single BIN's activity parameters. It is calculated against the total amount over four days. At the Issuer's option, it may **also** be applied to the total transaction count over four days.

This limit applies over a 4-day period. The 4-day count and amount limits are determined by multiplying the 1-day count and amount limits by the 4-day multiplier.

Note The 4-day multiplier is applied on a rolling basis so that as the next day arrives, in any 4-day period, the activity from the first day (expenditure and count) is no longer considered.

The multiplier can be any value between 1 and 4, in increments of 0.05 - if the result of the calculation is a non-integer value, the value is rounded up to the nearest integer.

28.3.7.1 Merchant category group activity limits

Activity limits, where enabled, are optional at MCG level.

28.3.7.2 Total purchase and total cash activity limits

It is mandatory to set activity limits for the transaction categories Total Purchase and Total Cash. VEAS defaults to these totals if limits have not been set for individual MCGs.

28.3.7.3 Issuer available and Issuer unavailable activity limits

Issuers can define separate limits for when an Issuer is available, and when an Issuer is unavailable. It is usual to set higher limits when the Issuer is unavailable.

The advantage of conservative available limits is greater risk control.

The disadvantage is increased transaction volume at the host for the relatively small number of transactions that exceed limits. Thus, Issuers may choose relatively conservative available limits.

The advantage of more liberal activity limits is that the Acquirer receives fewer decline responses. This reduction in traffic results in improved Cardholder service and less demand on the Issuer's customer service operations or referral centre.

The disadvantage is increased credit and fraud risk. However, because Issuer unavailable transactions should be relatively infrequent and difficult to predict, the fraud and credit risk lessens. For these reasons, Issuers may choose more generous Issuer available limits.

- Issuer available

If a STIP-processed transaction fails an activity limit check when the Issuer is available, VEAS forward-refers the transaction to the Issuer for approval.

- Issuer unavailable

If a STIP-processed transaction fails an activity limit check when the Issuer is unavailable, VEAS sends a decline response to the Acquirer (assuming no other STIP tests generate a higher priority response).

28.3.8 Mandated minimum limits

Visa mandates a number of Issuer and activity limits:

- VEAS does not apply mandatory minimum Issuer or activity limits to debit card or Prepaid card transactions.
- Issuers can request that their BINs be exempted from international mandatory minimum limits. However, exemption on Visa Premium products, such as Visa Gold card and above, are not recommended as these products must offer a level of service that is adequate to the Cardholder in situations where the risk is low and the need may be high. International mandatory minimum limits are targeted at the T&E sector for Cardholders who need to travel and eat internationally.
- Where an Issuer has gained exemption for a particular MCG, the Issuer's limit always takes precedence.

28.3.8.1 Mandatory minimum T&E Issuer limits

Visa Europe imposes a number of mandatory minimum Issuer limits (US dollars) for International Transactions within transaction type Travel & Entertainment (T&E transactions) when using Visa Classic card, Visa Gold card, and Visa Business card products. Other card products are not subject to these limits.

Table 36: Visa-mandated minimum Issuer limits for International Transactions

No.	Merchant category group	Classic	Business	Gold
1	Commercial Travel	USD 500.00	USD 750.00	USD 750.00
2	Lodging	USD 500.00	USD 750.00	USD 750.00
3	Auto Rental	USD 250.00	USD 350.00	USD 350.00

28.3.8.2 Mandatory minimum T&E activity limits

Visa Europe imposes a number of mandatory minimum Issuer limits (US dollars) for International Transactions within transaction type Travel & Entertainment (T&E), and Total Purchase when using Visa Classic card, Visa Gold card, and Visa Business card products. Other card products are not subject to these limits.

Table 37: Visa-mandated minimum 1-day activity limits for International Transactions: Issuer available

No.	Merchant category group	Classic	Business	Gold	1-day count	4-day multiplier
1	Commercial Travel	USD 500.00	USD 750.00	USD 750.00	2	2.00
2	Lodging	USD 500.00	USD 750.00	USD 750.00	2	2.00
3	Auto Rental	USD 250.00	USD 350.00	USD 350.00	2	2.00
	Total Purchase	USD 500.00	USD 500.00	USD 500.00	1	1.00

Table 38: Visa-mandated minimum 1-day activity limits for International Transactions: Issuer unavailable

No.	Merchant category group	Classic	Business	Gold	1-day count	4-day multiplier
1	Commercial Travel	USD 1,100.00	USD 2,200.00	USD 2,200.00	2	2.00
2	Lodging	USD 900.00	USD 1,750.00	USD 1,750.00	2	2.00
3	Auto Rental	USD 600.00	USD 900.00	USD 900.00	2	2.00
	Total Purchase	USD 1,000.00	USD 1,750.00	USD 1,750.00	3	2.00

28.3.8.3 Applying the appropriate Issuer or Visa-mandated minimum limits

When processing International Transactions for Visa Classic card, Visa Business card, and Visa Gold card products, VEAS uses (unless an MCG is exempted) the limit with the higher threshold amount.

Table 39: Issuer limits

Transaction type	Issuer-specified limit	Visa-mandated minimum limit	Use
T&E	lower	higher	Visa-mandated minimum limit
T&E	higher	lower	Issuer-specified limit

Table 40: Activity limits

Transaction type	Issuer-specified limit	Visa-mandated minimum limit	Use
T&E, Total Purchase	lower	higher	Visa-mandated minimum limit
T&E, Total Purchase	higher	lower	Issuer-specified limit

28.3.9 Activity checking

Activity checking only considers and accumulates approved transactions. It also excludes transactions below the advice limit, and items afforded a special status such as action code 11 (Very Important Person).

Important The following description of activity checking and accumulation assumes that the combination of Issuer specifications and transaction characteristics would result in activity checking, and that the transaction passed all other STIP tests.

Accumulators are running totals of transactions approved in STIP. While Issuers specify activity limits at the BIN level, VEAS maintains accumulators at the account level.

An accumulator is incremented only when a transaction passes all STIP tests, and STIP sends an approval response to the Acquirer. Transactions approved by the Issuer, including those forward referred to the Issuer by STIP, do not increment accumulators.

VEAS compares the activity accumulators to the appropriate Issuer available or unavailable limits. The same set of accumulators is used in both instances. Issuer available and Issuer unavailable activity checking differ in the following ways:

- The particular set of limits (available and unavailable) that are used
- The consequences of failing activity checking:
 - If the Issuer is available, forward refer to the Issuer
 - If the Issuer is unavailable, respond with a decline to the Acquirer

In all other respects, the same activity checking and accumulation rules apply:

- A transaction passes an activity check if adding it to an accumulator does not cause an accumulator to exceed its associated activity limit
- A transaction fails an activity check if adding it to an accumulator causes an accumulator to exceed its associated activity limit. STIP assigns one of the following response codes to an activity fail check:
 - Response code 65 (exceeds count limit)
 - Response code 61 (exceeds amount limit, or both count and amount limits)

Rules for passing and failing vary between MCGs.

Table 41: Pass and fail parameters for MCG activity checks

No.	Merchant category group	Activity limits	MM	Must pass
1	Commercial Travel	Optional	✓	Either MCG or Total Purchase
2	Lodging	Optional	✓	Either MCG or Total Purchase
3	Auto Rental	Optional	✓	Either MCG or Total Purchase
4	Restaurant	Optional		Either MCG or Total Purchase
5	MOTO	Optional		MCG and Total Purchase
6	Risky Purchase	Optional		MCG and Total Purchase
	Total Purchase	Required	✓	n/a
9	ATM Cash ATM Cash <= Total Cash ATM Cash > Total Cash	Optional		MCG and Total Cash ATM Cash
	Total Cash	Required		n/a

MM indicates a mandated minimum exists for International Transactions.

28.3.9.1 Travel & entertainment activity checking

If mandatory minimum limits apply, VEAS checks and accumulates activity using the greater of Issuer-defined or mandatory minimum activity limits.

If mandatory minimum limits do not apply, VEAS checks and accumulates activity using the Issuer-defined limits.

If MCG level activity limits do not apply, or if activity checking fails at the MCG level, VEAS checks and accumulates Total Purchase activity.

To fail activity checking, both MCG and Total Purchase limits must be exceeded.

28.3.9.2 Purchases: MOTO and risky purchase activity checking

If defined, VEAS checks and accumulates MCG level activity limits. If the Issuer has not defined specific MCG level limits, VEAS checks and accumulates Total Purchase activity limits.

Note MOTO contains STIP activity limits for internet-based transactions.

To pass activity checking, both the MCG and Total Purchase accumulators must remain within their defined limits.

28.3.9.3 Purchases: other purchase and medical activity checking

Issuer-defined, MCG level activity limits are not available for Other Purchase and Medical Merchant category groups. VEAS therefore checks and accumulates Total Purchase activity limits.

To pass activity checking, the Total Purchase accumulators must remain within their defined limits.

28.3.9.4 Cash: other cash and quasi-cash activity checking

Issuer-defined, MCG level activity limits are not available for Other Cash and Quasi-Cash Merchant category groups. VEAS checks and accumulates Total Cash activity limits.

To pass activity checking, the Total Cash accumulators must remain within their defined limits.

28.3.9.5 Cash: ATM cash activity checking

If MCG limits exist, VEAS checks and accumulates activity limits at the MCG level. If the Issuer has not defined specific MCG level limits, VEAS checks and accumulates Total Cash activity limits.

To pass activity checking, if the total is less than or equal to the Total Cash limit, both the MCG and Total Cash accumulators must remain within their defined limits. If the total is greater than the Total Cash limit, both the MCG and Total Cash accumulators must remain within their defined limits.

28.3.10 Cardholder risk levels and individual limits

Under normal PCAS processing, Members set up parameters at BIN level, which are used if any transactions go into STIP. All cards under the BIN use the same parameters.

The Risk File is a Cardholder Database file that resides on VEAS and enables Members to tailor their PCAS parameters to individual cards or groups of cards. When a transaction goes into STIP, Visa uses the parameters from the Risk File rather than the BIN level parameters.

There are 4 levels used under PCAS for Members to set parameters, levels A, B, C and D. Level A is designed for use with Cardholders which are regarded to be of least risk, and level D is designed for use with Cardholders who are regarded to be of most risk. The default setting for BINs is level C; and most Members set up PCAS parameters at this level.

The most basic way of using the Risk File is for Members to set PCAS parameters on one or more of the other levels A, B and D. Once this is done Members can then add cards to the risk level and point them at the appropriate level. This means that Cardholders assigned to the different groups use the parameters for those groups should their transactions go into stand-in processing.

Table 42: PCAS parameters in Risk File

Risk level	Description	Typical application
A	Generous parameters for low risk accounts	Premium or low risk accounts
B	Issuer defined risk level parameters	Accounts appropriate to the issuer-defined parameters
C	Visa Authorization default risk level. Established at BIN level	Medium risk or new accounts

Table 42: PCAS parameters in Risk File (continued)

Risk level	Description	Typical application
D	Established at account level only. Not subject to the mandatory minimum issuer limits or advice limits	High risk accounts

If Issuers want to specify more than one risk level, they must specify an Issuer limit for each Merchant category group (MCG) for each risk level. Activity limits specified at the BIN default level do not apply to accounts on the non-default risk levels.

Issuers can assign one or more of the following limits to each risk level:

- Issuer limits by MCG
- Activity limits by MCG
 - 1-day count and amount limits
 - 4-day multipliers
 - Issuer available and unavailable limits
- Between limits random selection factor
- Below advice limit random selection factor
- Between limits advice creation and activity checking options

Issuers can also establish Cardholder-specific activity limits in the exception file in the Cardholder Database, which can contain both positive and negative information in the form of action codes. These limits take precedence over risk level limits.

When limits are specified at multiple levels, VEAS uses the following hierarchy:

1. Account-specific limits
2. Risk level "D" limits
3. Mandatory minimum limits (when applicable and when greater than Issuer-specified limits)
4. BIN (default risk level) limits

Issuers assign accounts non-default risk levels by one of two methods:

- Encoding Track 1 in the magnetic stripe of the card when the Issuer issues the card
Visa does not recommend this method because a relatively high percentage of transactions do not contain Track 1 data.
- Adding an account to the risk-level file in the Cardholder Database (CDB)
Issuers can optionally use this method to override the risk level on the magnetic stripe.

A risk level specified in the risk level file takes precedence over a risk level encoded on the magnetic stripe. If the transaction data or the Cardholder Database does not specify a risk level, VEAS uses the default risk-level file parameters for the BIN.

28.3.11 Random selection factors

An Issuer can randomly select a percentage of STIP transactions for additional scrutiny. The process is weighted in favour of selecting higher-amount transactions in order to counteract authorization predictability based on transaction values alone.

Issuers can specify a separate random selection factor (a percentage 0%-30%) for transactions that are below the advice limit, and those that are between the advice and Issuer limits:

- Below the advice limit

STIP selects the specified percentage of transactions and processes them as if they were between the advice and Issuer limits. VEAS processes the remaining transactions as below the advice limit transactions.

When the advice and Issuer limits are equal, VEAS sends randomly selected below the advice limit transactions to the Issuer.

- Between the advice limit and Issuer limit

STIP selects the specified percentage of transactions and processes them as if they were above the Issuer limit. This means that they are either sent directly to the Issuer (if the Issuer is available) or authorized by STIP against the above Issuer limit conditions.

Random selection processing reduces fraud exposure by reducing the chance of predicting STIP authorizations.

28.3.12 BIN blocking, country restrictions, risky countries and country-to-country embargos

28.3.12.1 BIN blocking

Issuers can block entire BINs as well as certain transaction types. In addition to blocking an entire BIN, Issuers can block BINs for domestic cash transactions, international cash transactions, or both.

28.3.12.2 Country restrictions

At the BIN level, Issuers can specify that their cards are available for use:

- In all countries
- Only in the country of issuance
- Only in a selected list of countries
- In all countries except a selected list of countries

Excluded countries appear in the Country Exclusion table.

28.3.12.3 Risky countries

Issuers can specify that all requests originating in risky Acquirer countries be routed directly to them. Risky country transactions switched to the Issuer bypass mandatory minimum limits such as those for T&E transactions; and any Issuer-defined limits.

If an Issuer is unavailable, they can choose their regular STIP parameters with which to generate a response, or to decline all requests immediately.

The Risky Countries table can identify up to 20 countries as being high risk.

Note VEAS searches the Country Exclusion table before it searches the Risky Countries table. For countries appearing in both tables, the country exclusion processing specifications takes precedence.

28.3.12.4 Country-to-country embargos

VEAS maintains a Country-to-Country (embargo) table on behalf of local government.

In addition to using embargo settings for Visa cards, the settings can also be used for other card products such as American Express or MasterCard.

28.3.13 Suppress inquiry mode

Suppress inquiry (SI) mode enables Visa System Processors to control input and output message processing during heavy traffic periods. When a Processor assigns SI mode to a station, VEAS blocks all routine incoming authorization and reversal requests from entering that station. This enables the station to concentrate on processing outgoing requests.

When a Processor is in SI mode, VEAS cycles through all the Processor's stations until an available non-SI mode station is found. If all the Processor's stations are in SI mode, PCAS diverts low value/low risk transactions to STIP using Issuer unavailable limits. If limits are exceeded transactions are forward referred.

A Processor enters and exits SI mode using 0800 network management messages. The field 70 - Network Management Information Code sign-on code is 062; the sign-off code is 063.

28.4 Key data fields

The following key data field is used by the PCAS. For detailed information, see the Visa Europe technical specifications.

Data field 44.1 - Response Source/Reason Code

This data field contains a code that identifies the source of the field 39 - Response Code decision. The response source will be either the Issuer or STIP.

29 Priority Routing Service

For Single Message System (SMS) processing, the rules by which any individual transaction is processed are determined by its network identification code. One card may be eligible for a number of possible schemes, and therefore a number of different network identification codes may be possible. Acquirers that use SMS choose which rules and which network identification code are appropriate for each transaction and must include the network identification code in the financial request message.

For Acquirers that use SMS and accept transactions destined for either the Visa or Plus networks, the Priority Routing Service can simplify the task of assigning a network identification code. This is achieved by delegating to the Visa Europe Authorization Service (VEAS) the authority to determine the preferred network and the set of programme rules to use for each transaction. Acquirers can request priority routing only for authorizations, status-check authorizations, original credit transactions, and original financial transactions and their reversals.

Acquirers do not assign a specific network identification code in the authorization request, but enter a value of 0000 in the network identification code data field of the request (subfield 63.1). When VEAS identifies a 0000 value, it automatically determines which network and card programme rules apply.

29.1 Related information

For further information about the Priority Routing Service, see the following documents:

- *Introducing the Visa Europe System*
- *Introducing the Visa Europe Authorization Service*
- *Introducing Single Message System (SMS) and Dual Message System Authorization (DMSA) Transactions*
- *Introducing Single Message System (SMS) and Dual Message System Authorization (DMSA) Messages*

29.2 Participation

The Priority Routing Service is available through the single message system.

Participation is optional for Acquirers that use SMS and their Processors.

Note Dual Message System Authorization (DMSA) messages are required to contain a network identification code. Acquirers must populate subfield 63.1 with 0000 and VEAS subsequently selects an appropriate value. In this respect, the Priority Routing Service is a mandatory requirement for Acquirers that use DMSA.

To participate in the service, Members must meet the following requirements.

29.2.1 Testing and certification

Certification is mandatory to participate in the service. The VisaNet Certification Management Service (VCMS) provides testing and certification assistance for Priority Routing Service participants. Members should contact Visa Europe Customer Support for advice and assistance on the appropriate testing and certification requirements.

29.2.2 Planning and implementation

Acquirers using the Priority Routing Service must comply with the most stringent data field requirements of all networks in which it participates.

If an Acquirer participates in the Visa and Plus networks and a given data field is mandatory for Visa but conditional for Plus, the mandatory requirement takes precedence.

29.3 How the service works

There are two networks through which transactions can be routed: Visa and Plus. The Priority Routing Service enables the Acquirer to let VEAS determine which network and card programme rules to use for a transaction.

On a weekly basis, Members receive from Visa Europe account range tables of active (Visa and Plus) card programmes. These identify the networks and account programmes that apply to the relevant account number ranges. Acquiring Members therefore have the information needed to route authorization requests to VEAS and, if they wish, assign the network identification code. Acquirers must ensure that the network identification code they select is one in which both they and the Issuer participate.

To use the Priority Routing Service, an Acquirer does not enter a specific network identification code in the request, but enters a value of 0000 in subfield 63.1.

When VEAS receives an authorization request with 0000 in subfield 63.1, VEAS selects the appropriate network and card programme rules and assigns a network identification code to the authorization request. VEAS always prioritises the Visa network over the Plus network. For example:

- A transaction that uses a card with the Plus mark is automatically routed to the Visa network.
- A transaction that uses a MasterCard with the Plus mark is automatically routed to the Plus network.
- Acquirers that use SMS and participate in the Priority Routing Service can override automatic network selection and assign a network identification code to the request before they forward it to VEAS. For example, a transaction that uses a Visa card with the Plus mark is routed to the Plus network if the Acquirer assigns the Plus network identification code to the request. Acquirers that use DMSA must populate subfield 63.1 with 0000.

The authorization request is then forwarded to the Issuer that performs authorization and returns the authorization response with the appropriate network identification code to VEAS. VEAS then forwards the authorization response to the Acquirer.

29.4 Process flows

The process flow for the Priority Routing Service is:

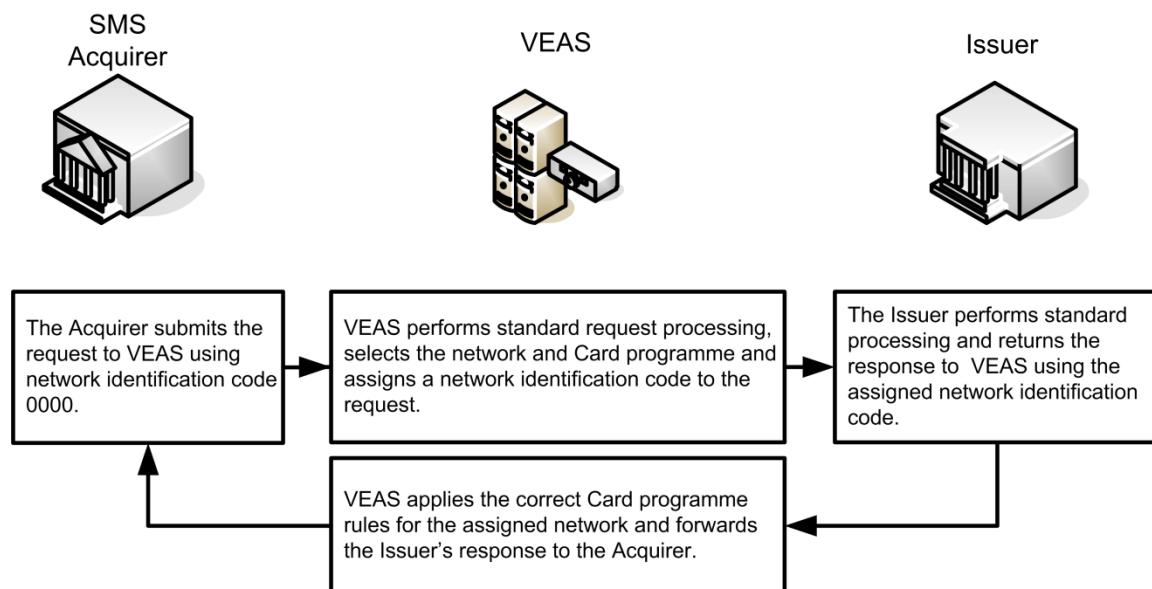
1. The participating Acquirer enters the value 0000 in subfield 63.1 of the authorization request to activate automatic network selection.
2. VEAS assigns the appropriate network identification code and forwards the authorization request to the Issuer with only those fields that apply to the network's programming rules.
3. The Issuer processes the authorization request and returns the authorization response to VEAS.
4. VEAS forwards the authorization response and the assigned network identification code to the Acquirer.

Important If the Acquirer requests priority routing for a transaction, each field in each message must comply with all of the field requirements for all of the card programmes that are supported by that Acquirer.

Further processing must comply with any programme rules that are associated with the specified network.

The following diagram illustrates the process flow for the Priority Routing Service.

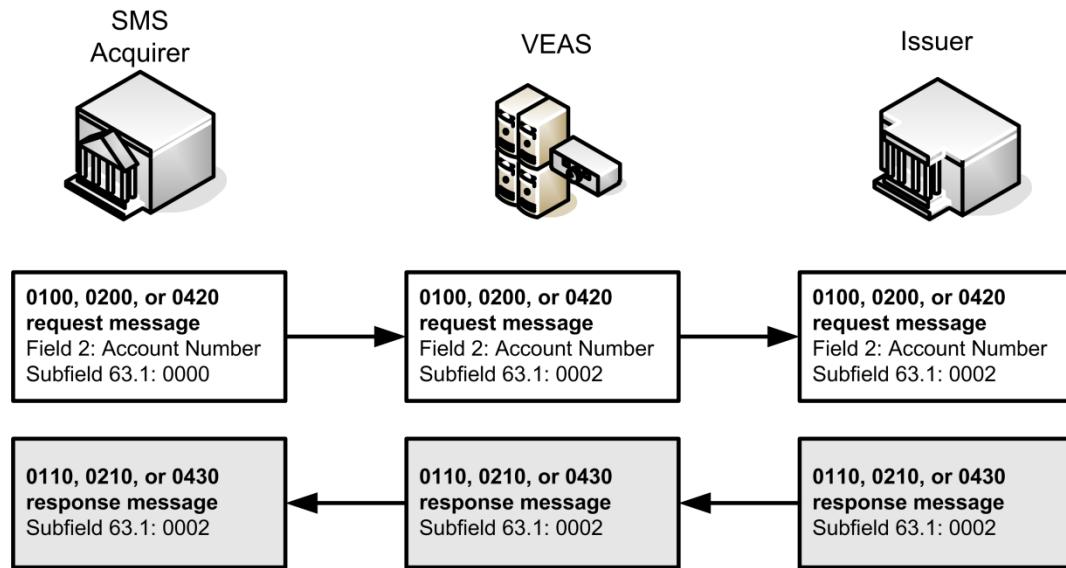
Figure 63: Process flow for the Priority Routing Service



29.5 Message flows

The following diagram illustrates the message flow for the Priority Routing Service.

Figure 64: Message flow for the Priority Routing Service



29.6 Key data fields

The following key data fields are used by the Priority Routing Service. For detailed information, see the Visa Europe technical specifications.

Data field 2- Primary Account Number (PAN)

This data field contains the account number that is used to determine the routing. Data field 2 is used in any message that is related to a transaction and in 0302 and 0312 file maintenance messages.

Note Data field 100- Receiving Institution Identification Code takes priority over data field 2 if the Acquirer provides both fields.

Data field 63.1 - Network Identification Code

This subfield contains a value that specifies the network that VEAS is to use for transmitting the message. The network determines the programme rules that apply to the transaction.

30 Real Time Scoring Service

The Real Time Scoring (RTS) Service enables Issuers to subscribe to one of two options:

- **Score only:** This option enables Issuers to receive a risk score and, optionally, a risk indicator in the authorization requests they receive. The score indicates the risk of fraud and the risk indicator indicates a compromised card.
- **Full solution:** In addition to the above features, this option gives Issuers access to the Case Manager application via Visa Online. Case Manager enables Issuers to generate cases for risky transactions that can be evaluated by an analyst. On subscription, Issuers provide a set of rules that they want transactions to be evaluated against. Cases are created either because of high scores and/or because a transaction satisfies the criteria of a rule.

Issuers can also select from options that enable them to receive risk scores and decision recommendations at the time authorization requests are received. A further option enables RTS to reach authorization decisions on the Issuer's behalf, based on rules written and managed by the Issuer.

30.1 Related information

For further information about RTS, see the following documents:

- *Visa Europe Real Time Scoring Member Implementation Guide*
- *Visa Europe Real Time Scoring Case Manager User Guide*
- *Visa Europe Real Time Scoring Rules Manager User Guide*
- *Visa Europe Real Time Scoring - Authorization Decision Recommendations Quick Reference*

30.2 Participation

RTS is available through the dual messaging system.

Participation is optional for Issuers and Processors.

To participate in RTS, testing and certification is required for Issuers that choose either of the following:

- Score only solution
- RTS full solution with options that result in receiving information that affects authorization requests (for example, risk scores and/or authorization decision recommendations)

Testing and certification are not required for Issuers that choose the RTS full solution and that do not choose to receive information that affects authorization requests. For these Members, no system changes are required, as RTS is a Visa Europe-hosted solution, accessible through a web browser.

For more information on implementing this service, contact Visa Europe Customer Support.

30.3 How the service works

RTS offers Issuers the following solutions.

Table 43: RTS solutions

Option	Description	Suitable for	System modification required?
Score only	Issuers receive the risk score in the incoming authorization request.	Issuers that want to use scoring in combination with their own fraud detection systems to approve, refer or decline authorization requests.	Yes
Full solution	Issuers have access to the RTS case management capability, which enables Issuers to view cases created in real time via a web browser. The cases are derived from fraud detection rules maintained by the Issuer. Also includes options for real-time scoring, authorization recommendations and decision-making.	Issuers that want flexibility as to the RTS options they select and/or that want Visa Europe to be responsible for authorization decision advice or actual decision-making.	No (unless Issuers want to receive the risk score or authorization decision recommendations in authorization requests)

For both solutions, an additional option enables Issuers to receive indicators (risk score reason codes) in the authorization request, which highlight abnormal conditions, for example, suspect ATM, compromised card.

30.3.1 Using the score only option

For Issuers that choose the score only RTS option, the main steps in using RTS are:

1. The Acquirer sends a transaction to VEAS.
2. VEAS forwards the transaction to RTS.
3. RTS sends the risk score back to VEAS.
4. VEAS sends an authorization request, including the risk score, to the Issuer.
5. The Issuer receives the risk score in the authorization request and uses this information to decide whether to approve, decline or refer the transaction.

30.3.2 Using the Real Time Scoring full solution

For Issuers that choose the RTS full solution, the main steps in using RTS are:

1. The Acquirer sends a transaction to VEAS.
2. VEAS forwards the transaction to RTS.
3. RTS generates a pre-authorization risk score.
4. VEAS sends the authorization request to the Issuer.
5. The Issuer receives the authorization request. Depending on the options chosen by the Issuer, they may receive the risk score and, optionally, the decision recommendation in the authorization request. The Issuer performs their normal checks and approves, declines or refers the transaction.
6. RTS Case Manager generates a post-authorization risk score.
7. If either the pre-authorization risk score or the post-authorization risk score and/or the rules created and maintained by the Issuer indicate that the transaction is sufficiently risky, Case Manager creates a case.
8. After sending the authorization response, the Issuer can view the case in Visa Online (Visa's secure, Internet-based communications channel).

For a description of the options that are offered under the RTS full solution, see [Process flow for the RTS full solution option](#) on page 253.

30.4 Process flows

The following process flows for RTS are illustrated in this section:

- Score only
- Full solution (including Rules Manager)

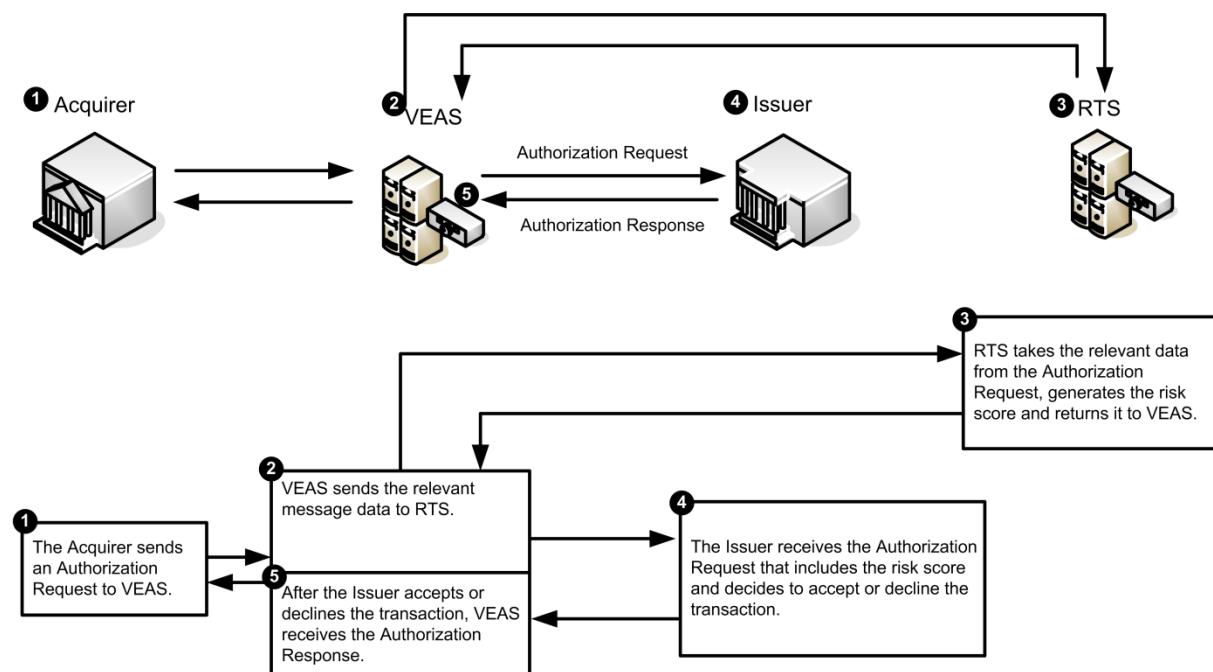
The additional options for the RTS full solution, which can be selected if required, are:

- Risk score
- Authorization decision recommendations
- Authorization decision-making

30.4.1 Process flow for the RTS score only option

The following diagram illustrates the process flow for the RTS score only option.

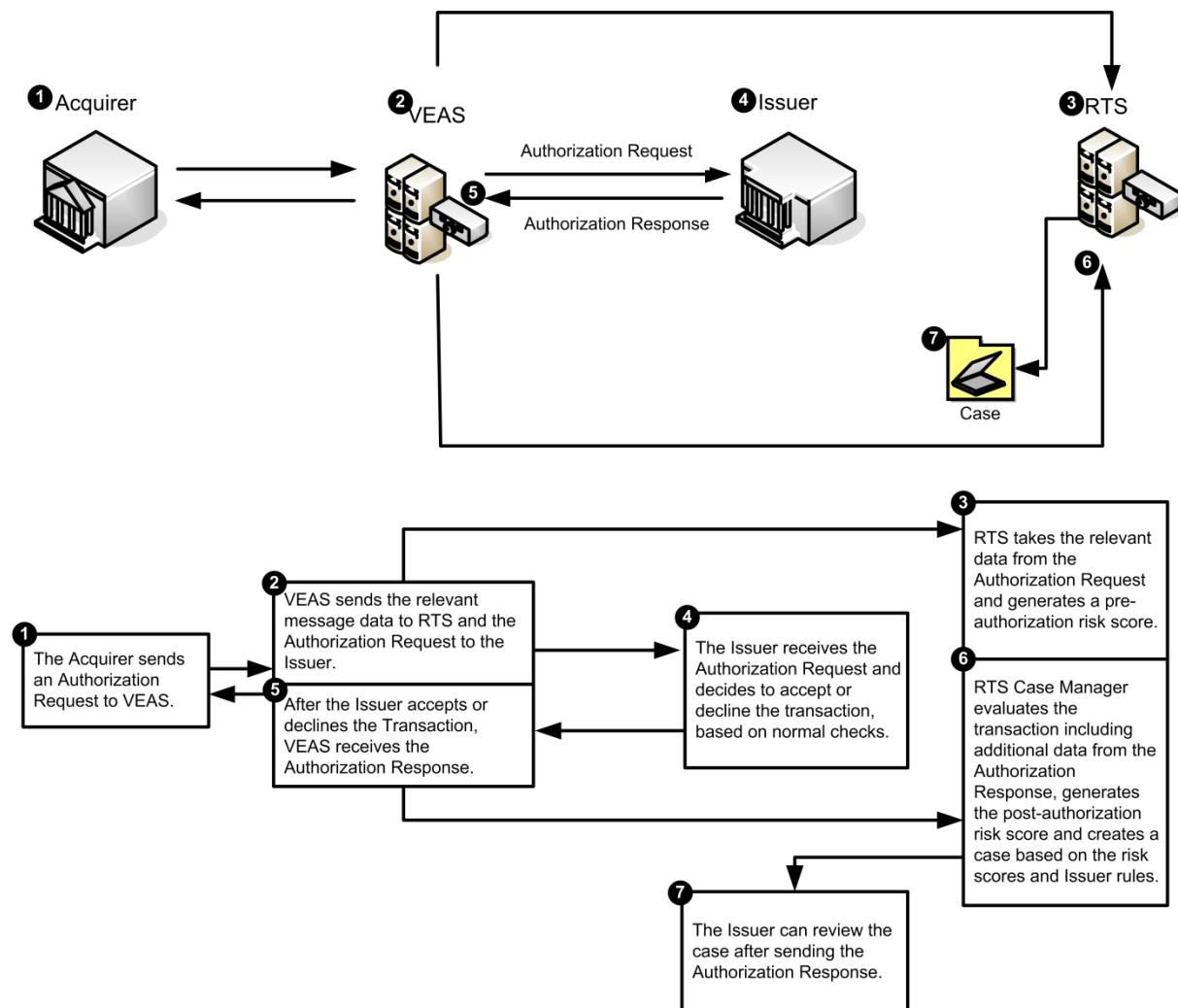
Figure 65: Process flow for the RTS score only option



30.4.2 Process flow for the RTS full solution option

The following diagram illustrates the process flow for the RTS full solution.

Figure 66: Process flow for the RTS full solution



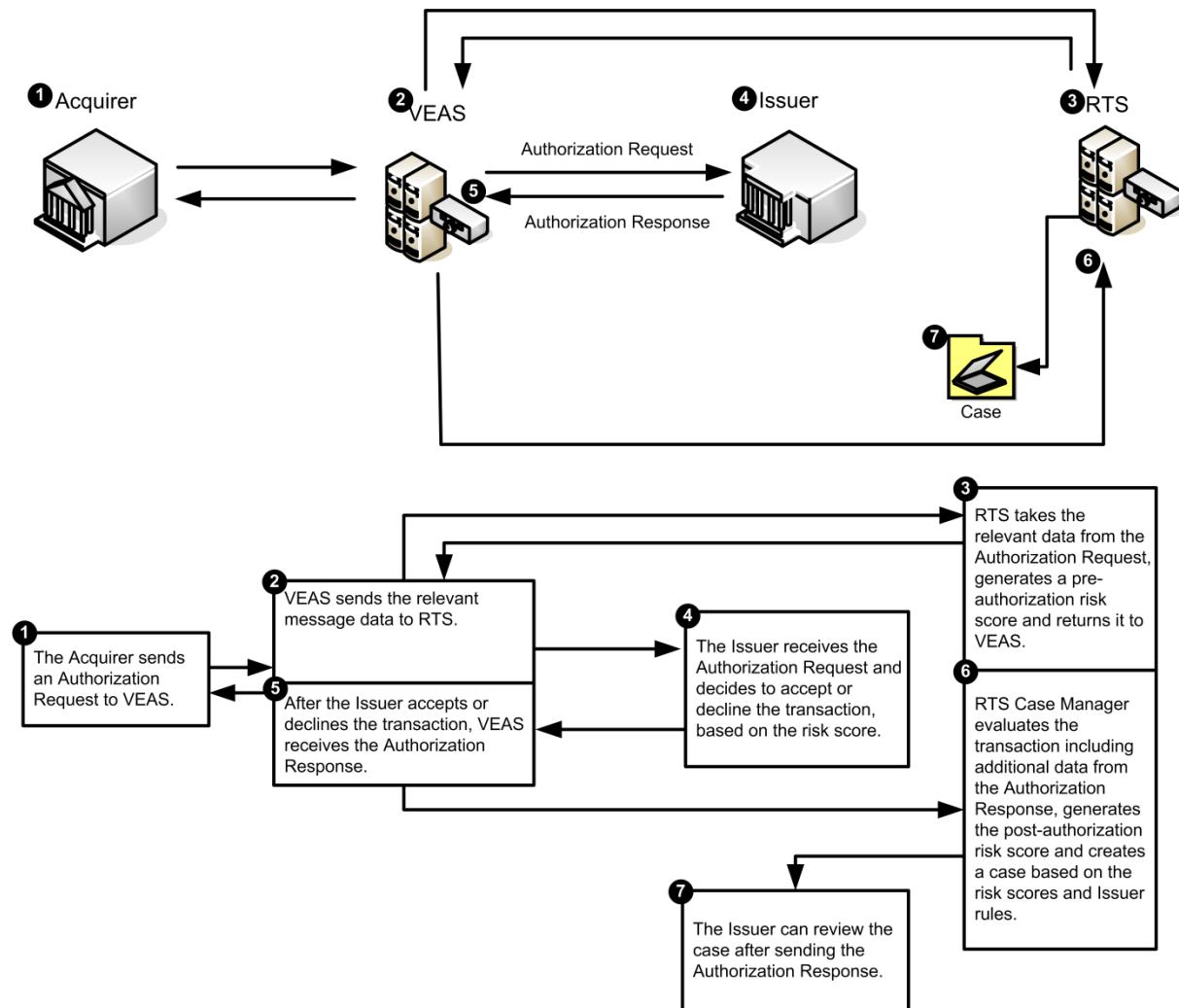
Issuers that choose the full solution can also select other options, including some or all of the following:

- [RTS full solution with risk score](#) on the next page
- [RTS full solution with decision recommendations](#) on page 255
- [RTS full solution with authorization decision-making](#) on page 256

30.4.2.1 RTS full solution with risk score

The following diagram illustrates the process flow for the RTS full solution, including the risk score option.

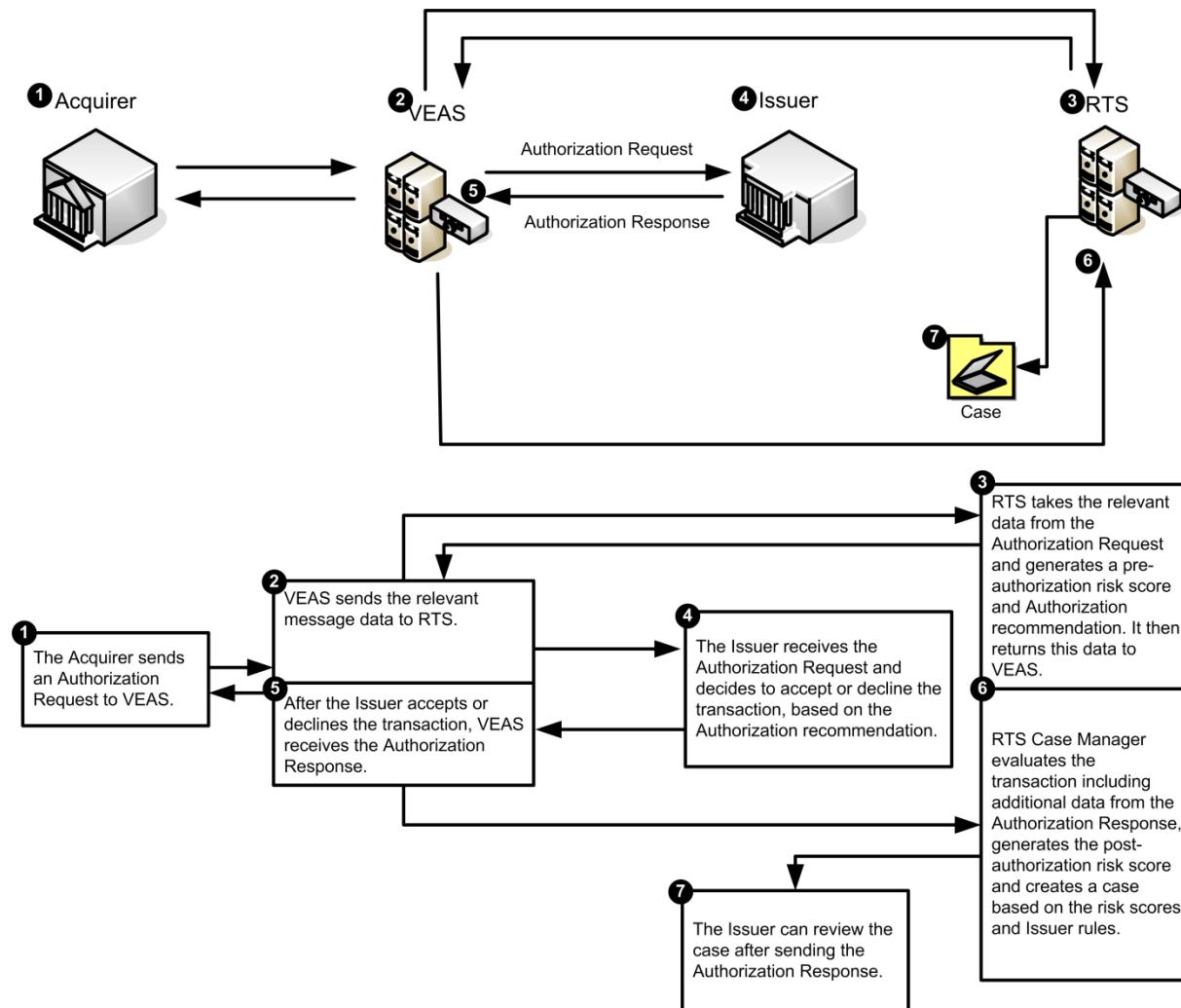
Figure 67: RTS full solution with risk score



30.4.2.2 RTS full solution with decision recommendations

The following diagram illustrates the process flow for the RTS full solution, including the option for RTS authorization decision recommendations.

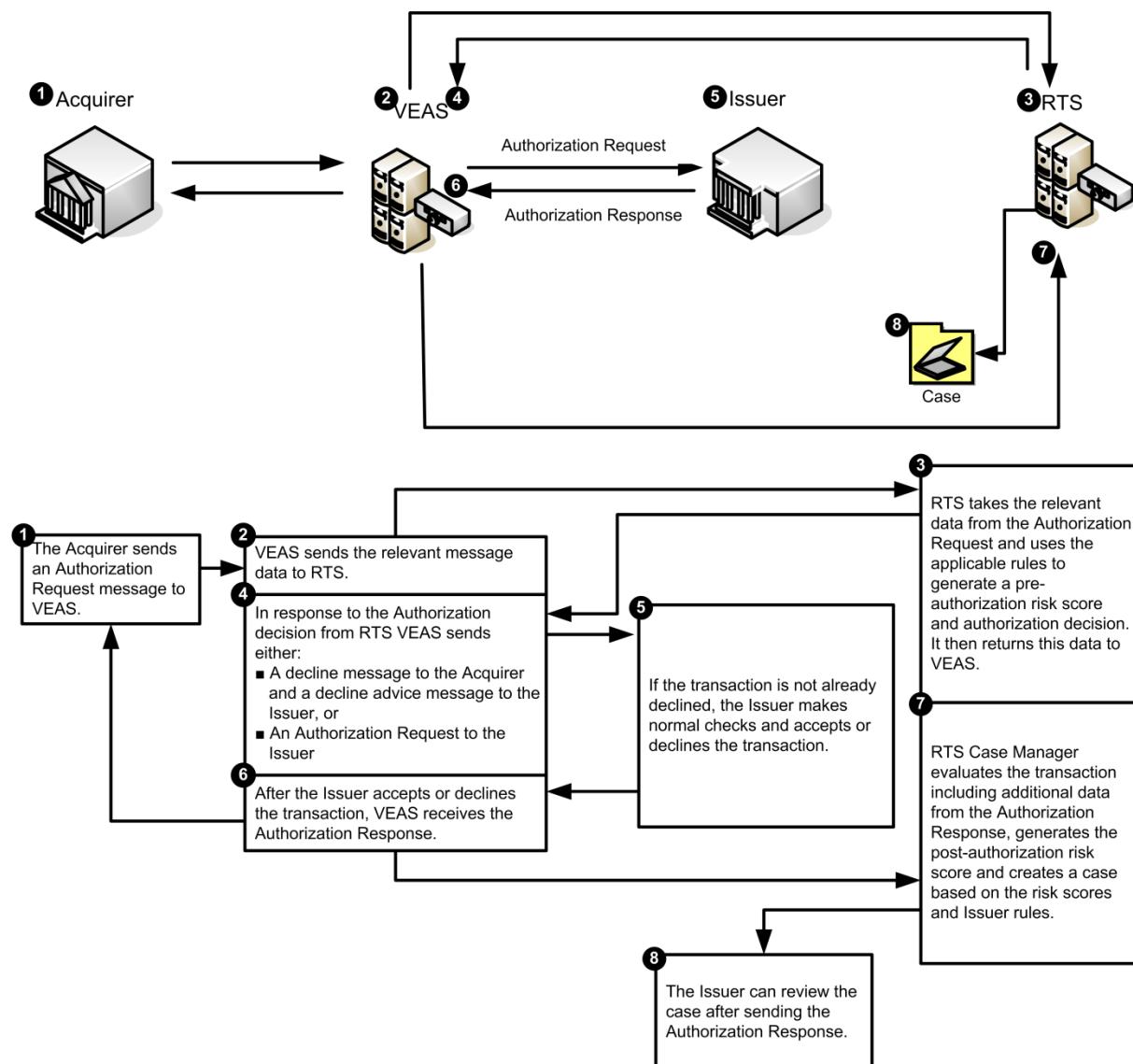
Figure 68: RTS full solution with decision recommendations



30.4.2.3 RTS full solution with authorization decision-making

The following diagram illustrates the process flow for the RTS full solution, including the option for RTS authorization decision-making.

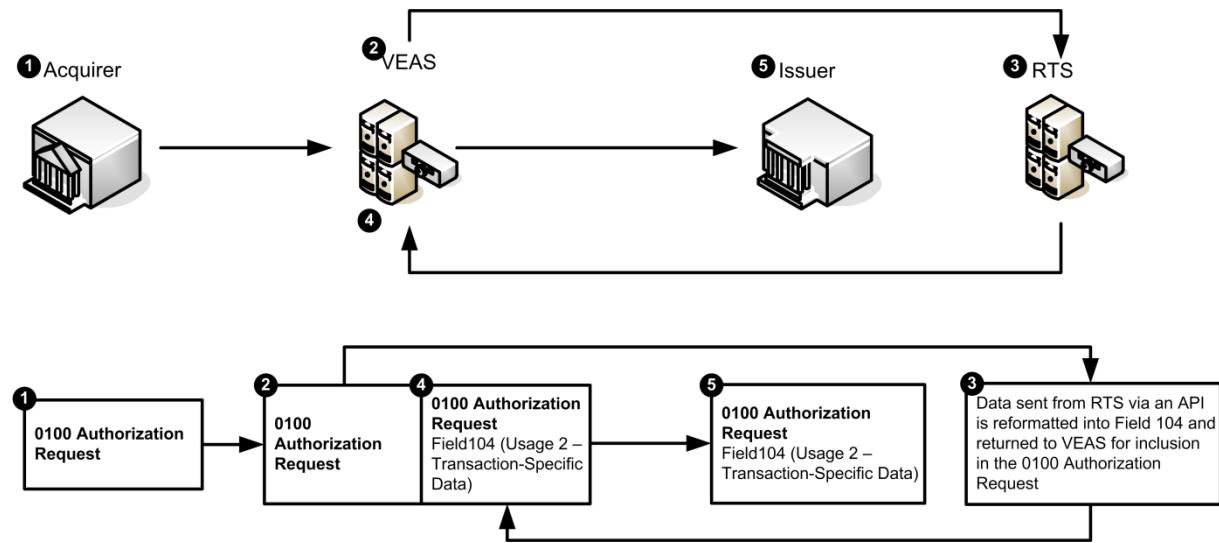
Figure 69: RTS full solution with authorization decision-making



30.5 Message flows

The following diagram illustrates a simplified version of the message flow for RTS (Risk Scoring option only).

Figure 70: Message flow for the RTS service



30.6 Key data fields

The following key data field is used for RTS.

Data Field 104, Usage 2 - Transaction-Specific Data, dataset ID 64 (Visa Europe Real Time Scoring data)

The risk score is represented by a numeric value from 000 to 999, with a higher score representing a greater risk.

31 Verified by Visa Service

Verified by Visa (VbV) reduces card-absent fraud in e-commerce environments by enabling Issuers to verify that the Person making the purchase is an authorized Cardholder. This verification process is called payment authentication.

VbV improves both Cardholder and Merchant confidence in internet purchases and helps to reduce disputes and fraudulent activity related to the use of Visa cards. Issuers can benefit from reduced costs associated with the most common types of internet disputes.

The Verified by Visa mark is displayed to the Cardholder during registration and each time the Cardholder enters a password for authentication at the time of purchase, and may also be displayed by participating Merchants.

The authentication method is called 3-D Secure; the authentication service available to Cardholders is called VbV. The Cardholder Authentication Verification Value (CAVV) is a cryptographic value the Issuer generates and sends to the Merchant during the authentication process in a VbV transaction.

Payment authentication gives Issuers the ability to authenticate Cardholders during an online purchase or e-commerce authorization transaction to:

- Reduce the likelihood of fraudulent usage of Visa cards
- Improve transaction performance to benefit all participants

It involves two phases:

1. VbV
2. CAVV generation

In the second phase, the Access Control Server (ACS) of the Issuer authenticates the Cardholder and generates a CAVV that it associates with the purchase. The CAVV generation is part of the suite of functions provided by VbV.

VbV enables all parties in an e-commerce payment transaction:

- To transmit confidential payment data
- To provide authentication that the Cardholder is an authorized user of a particular card

VbV is a global programme that supports magnetic-stripe Visa cards, Visa Smart Debit/Smart Credit (VSDC) cards and contactless cards.

It also supports a variety of Internet access devices including, but not limited to:

- Personal computers
- Mobile phones

The Visa Europe Authorization Service (VEAS) or the Issuer validates the results of authentication during authorization.

31.1 Related information

For further information about the VbV Service, see the following:

- *Dual Message System Authorization (DMSA) Technical Specifications*
- *Single Message System (SMS) ATM Technical Specifications*
- *Single Message System (SMS) POS Technical Specifications*
- *3-D Secure System Overview*
- *3-D Secure Protocol Specification Core Functions*
- *3-D Secure Functional Requirements: Access Control Server*
- *3-D Secure Functional Requirements: Merchant Server Plug-in*
- *3-D Secure Service Specification: Authentication History Service*
- *3-D Secure System and Compliance Testing Facility User Guide*
- *3-D Secure Security Requirements: Enrollment Servers and Access Control Servers*
- *Member Implementation Guide (MIG) for Issuers*
- *Member Implementation Guide (MIG) for Acquirers/Merchants*

31.2 Participation

Participation in VbV is optional for Issuers and Acquirers that have e-commerce Merchants.

The VbV Service is available to all Members processing point-of-sale and point-of-service (POS) e-commerce transactions that involve Visa and Visa Electron.

To participate in the service, Members must meet the following requirements.

31.2.1 Issuer requirements

Issuers that participate in the VbV Service must be able to:

- Select VbV and CAVV validation standard mode and stand-in processing (STIP) processing options for authentication transactions, attempt transactions, or both
 - Submit to Visa Europe the CAVV Data Encryption Standard (DES) keys, as required
- Note** CAVV DES keys are required if Issuers want Visa Europe to validate the CAVV on their behalf. If Issuers do their own CAVV validation, the CAVV DES keys are not required.
- Modify their systems to support the required VbV data fields
 - Complete any regional requirements and forms

Issuers that wish to participate in the VbV Service should work with Visa Europe Customer Support to establish CAVV DES keys and parameters.

31.2.2 Acquirer requirements

Acquirers that participate in VbV Service must be able to:

- Submit the required VbV data fields in VEAS messages
- Modify their systems to receive data subfield 44.13 - CAVV Results Code

31.2.3 Testing and certification

The Visa Member Testing Service (VMTS) enables Members to test and certify their systems for the VbV Service. The testing includes the following:

- Unit testing
- Other internal testing (such as regression, stress, and QA)
- Product Integration Testing

Testing and certification are mandatory to participate in the service.

Participants must be certified to send or receive the following data subfields:

- 44.13 - CAVV Results Code
- 60.8 - Additional POS Information - Mail/Phone/Electronic Commerce and Payment Indicator
- 126.8 - Transaction Identifier (XID)
- 126.9, Usage 2 or 3 - 3-D Secure CAVV or 3-D Secure CAVV, Revised Format

To arrange for testing and certification, Members must contact Visa Europe Customer Support.

31.2.4 Service monitoring

Service monitoring is not available for the VbV Service.

31.2.5 Planning and implementation

This section describes the requirements for implementing the VbV Service. Requirements for Issuers, Acquirers and Merchants are listed.

31.2.5.1 Issuer implementation of VbV

The Issuer requires the following to implement the VbV Service:

- Issuer ACS
- Issuer Registration Server (RS)
 - Note** The Registration Server is not necessarily a separate server. Registration functionality may be provided by the ACS.
- Attempts Access Control Server (AACs)

There are two methods of implementing the VbV Service for Issuers:

- Develop their software
- Obtain software from a Vendor

Visa Europe offers two CAVV validation processing options to Issuers that participate in the VbV Service:

- Authentication
The Issuer is a full participant in the service and has Cardholders enrolled in the VbV Service. Visa Europe classifies transactions as authentication transactions when the Acquirer, the Issuer and the Cardholder all participate in the VbV Service and when the Cardholder authentication has been completed successfully.
- Attempt
The Issuer generates a CAVV for attempted transactions. CAVV Attempt validation is used when there is no Cardholder authentication but the Issuer ACS or their AACS server generates a CAVV value for PARes=A transactions. With Attempt transactions, the Issuer still participates in the VbV Service.

Both Authentication and Attempt allow Issuers to select one of the following predefined processes by which Visa Europe processes their transactions in standard mode and during STIP:

- Option 1: (V) VEAS does CAVV validation and declines should it fail
With this option, VEAS performs all validations on the Issuer's behalf, declines transactions when the CAVV validation fails, and forwards the status results of transactions that VEAS did not decline to the Issuer.
- Option 2: (F) All CAVV results to Issuer
With this option, VEAS performs all validations on the Issuer's behalf and forwards all status results of transactions to the Issuer.
- Option 3: (I) Issuer does its own CAVV validation
With this option, VEAS forwards the transactions to the Issuer to perform validation. The Issuer returns the status results in the response message.

31.2.5.2 Acquirer implementation of VbV

The Acquirer requires the following to implement the VbV Service:

- MPI (also referred to as Merchant server software)

Visa International provides the following as part of the interoperability of the VbV Service:

- Visa Directory Server
- Authentication History Server (AHS)

31.2.5.3 Merchant implementation of VbV

Merchants using the VbV Service must:

- Operate software to support the VbV Service. This software is referred to as a Merchant Plug-in (MPI).
- Develop and implement its own MPI or obtain technology products and consulting services (including software integration into the Merchant's commerce environment) from a technology provider.
- Display the VbV mark to communicate participation to their Cardholders.

To arrange implementation, Members must contact Visa Europe Customer Support.

31.3 How the service works

This section describes underlying concepts that are involved in VbV processing.

VbV transactions are initiated via the MPI and the Verify Enrolment Request (VEReq) messages sent via the Visa Directory Server. VEAS is used when the VbV transaction is submitted for authorization.

31.3.1 Linking three domains

VbV is based on the 3-D Secure protocol. This system transmits secure computer messages between the relevant parties during an e-commerce transaction to authenticate all the parties involved. There are three domains involved in each transaction (hence 3-D):

31.3.1.1 Issuer (includes the issuing bank and the Cardholder)

An Issuer can have their own ACS (where the card numbers and Cardholder information is stored) or have a Payment Service Provider (PSP) to authenticate cards on their behalf.

31.3.1.2 Acquirer (includes the Merchant and the acquiring bank)

An Acquirer can have their own MPI system or use a Processor. This is where the acquiring bank defines procedures to ensure the validity of the Merchant and where the process is initiated.

31.3.1.3 Interoperability

There are two interoperability domains:

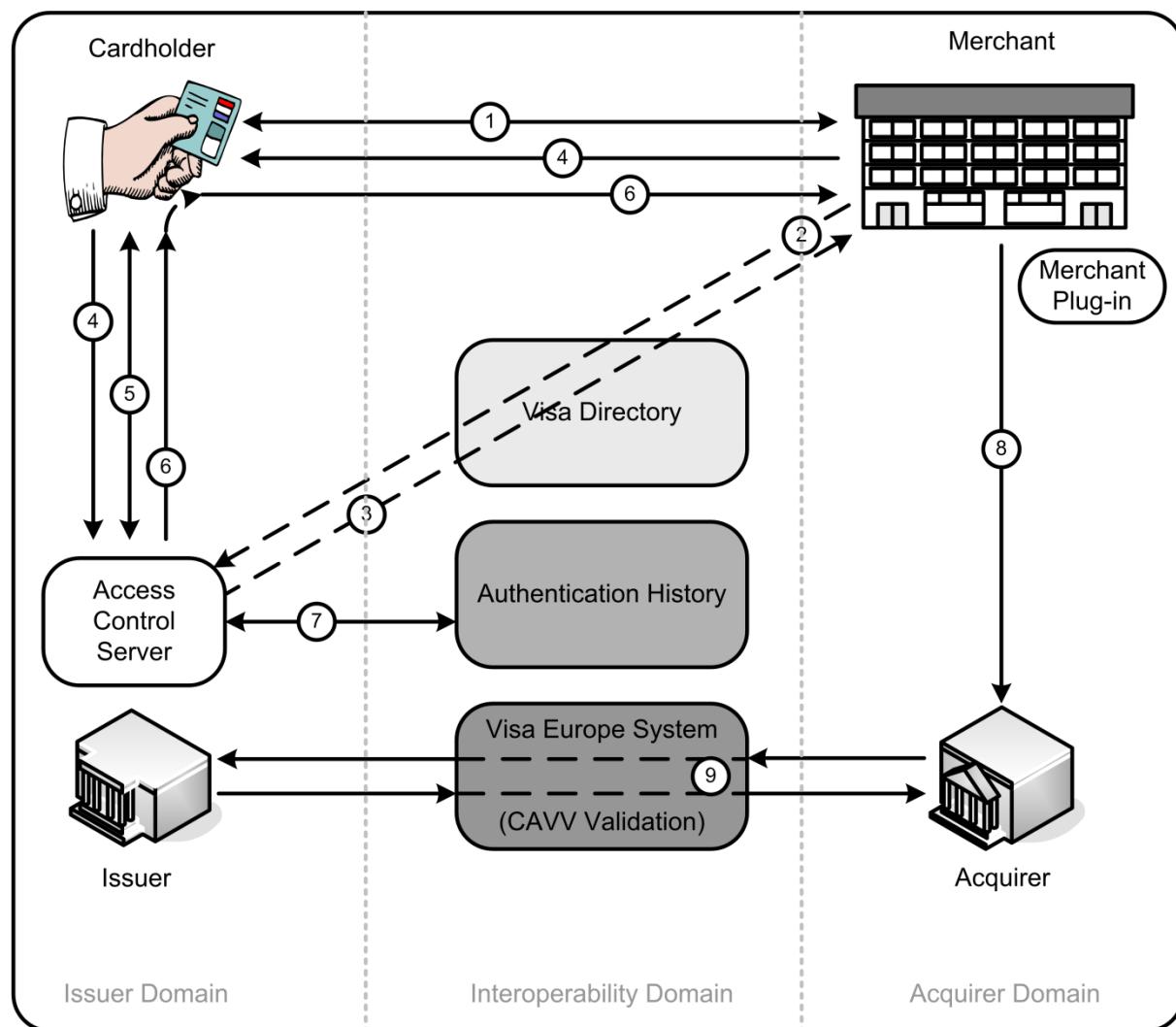
- Visa Directory Server
- Authentication History Server (AHS)

VbV operates various authentication methods such as dynamic passcodes and digital certificates. The Cardholder's issuing bank selects the approach.

31.4 Process flow

The following diagram illustrates the steps involved in a VbV authentication for an e-commerce transaction. Each step is explained below, with the numbered points below the diagram corresponding to the numbers on the arrows in the diagram.

Figure 71: Process flow for the Verified by Visa Service



The main steps in the VbV Service are:

1. The Cardholder enters a Merchant site, selects a product to purchase, enters details for payment including card number and submits the payment.
 2. The MPI contacts the Visa Directory Server to check if the card number is enrolled or is eligible to be enrolled in the VbV Service. The Visa Directory Server checks that the Merchant is genuine by verifying against details held and then sends the Verify Enrolment Request (VEReq) to the Issuer's ACS.
 3. The Issuer's ACS responds with a Verify Enrolment Response (VERes) to the Merchant MPI via the Visa Directory Server to confirm that the card number is enrolled or eligible to be enrolled, and that authentication is available. A URL is included in this response
- Note** MPI refers to VbV software that is integrated into a Merchant's website.

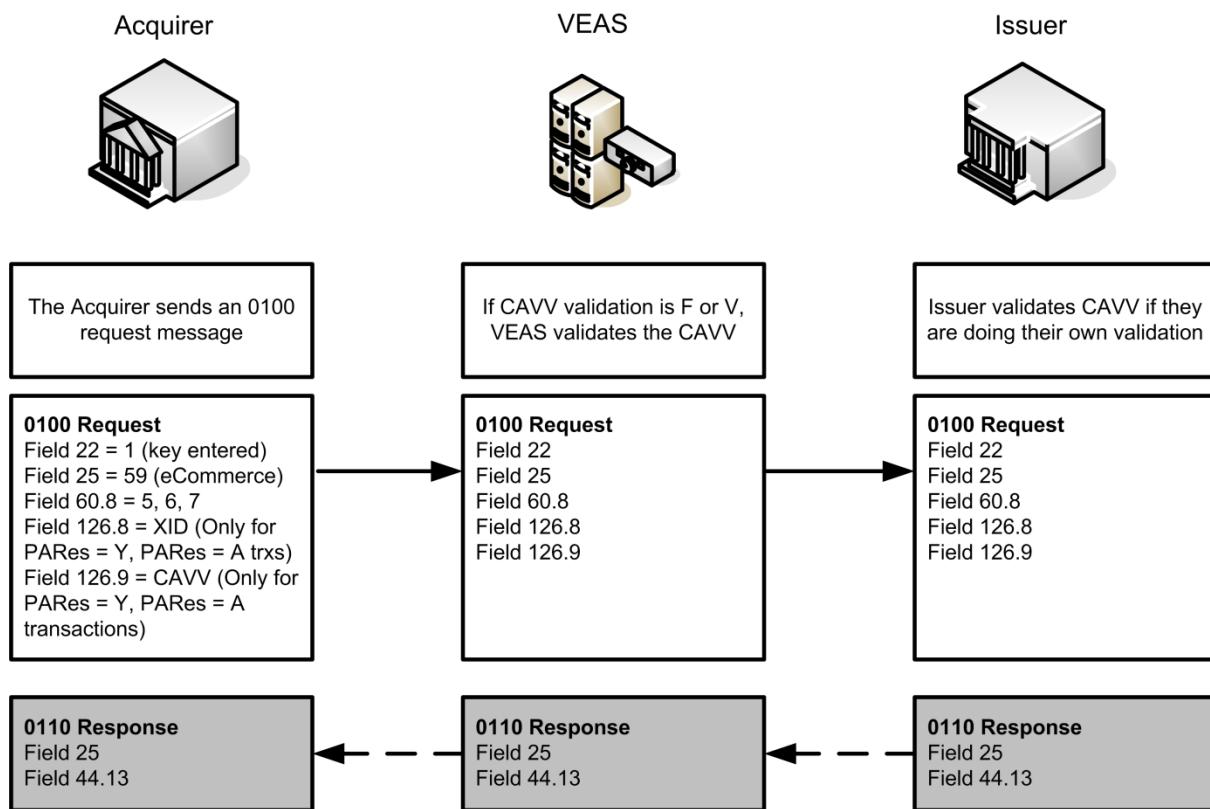
for a secure page to which the Cardholder's browser can be redirected for authentication.

4. If the card number is enrolled, the MPI sends a Payer Authentication Request (PAREq) to the location received in Step 3, for the Cardholder to confirm their identity. If the card number is not enrolled, but is eligible to be enrolled, the MPI redirects the Cardholder to the Activation During Shopping (ADS) page.
Note The ADS page is the Issuer's authentication window that is displayed on a Merchant's website during a VbV transaction.
5. The Issuer authenticates the Cardholder, using the authentication method selected by the Issuer.
6. The Issuer sends the Payer Authentication Response (PARes) (which contains the result of the authentication process) back to the Merchant.
7. The ACS sends a Payer Authentication Transaction Request (PATransReq) and Payer Authentication Transaction Response (PATransRes) to the AHS to assist with resolving disputes between Members.
8. Depending on the result of the authentication process, the Merchant sends the 'normal' authorization request via the Merchant's acquiring bank to the Issuer. A CAVV is available in authorization messages only when the PARes equals Y or A. VbV uses the CAVV to verify that the Cardholder is the rightful owner of the card. The CAVV is a cryptographic value generated by the Issuer and sent to the Merchant during the authentication process. The CAVV validation verifies that the CAVV submitted by an Acquirer in a VbV authorization message matches the CAVV generated by the Issuer, further strengthening security.

31.5 Message (authorization) flow

The following diagram illustrates the authorization message flow for the VbV Service.

Figure 72: Message (authorization) flow for the Verified by Visa Service



If both the Issuer and Acquirer have implemented the VbV Service then the following steps occur:

1. The Acquirer submits 0100 authorization request to VEAS as per the regular transaction process; however this contains the XID and CAVV data in fields 126.8 and 126.9 respectively.
2. VEAS performs one of a number of activities on receipt of these fields:
 - VEAS drops data subfields 126.8 and 126.9 from the authorization message if the Issuer PCR is not activated to receive this
 - Depending on Issuer's CAVV validation options VEAS either validates the CAVV value and return data subfield 44.13 to the Acquirer or sends the 0100 to the Issuer to validate the CAVV and return data subfield 44.13
3. The Issuer makes an authorization decision based on the CAVV validation, as well as the other transaction components and returns this in the 0110 message.
4. Whether the CAVV was validated by VEAS or the Issuer, the Issuer must submit a CAVV results code in data subfield 44.13 for informational purposes to the Acquirer. If the CAVV validation option is F (VEAS does the CAVV validations and forwards the result to the Issuer in the authorization message) and the Issuer does not return the CAVV result code, VEAS still sends the CAVV result code to the Acquirer.

31.6 Key messages

The following message types carry VbV data fields when using the VbV Service:

- 0100 authorization request
- 0110 authorization response
- 0200 financial request

The following messages are also involved in the VbV Service.

31.6.1 Verify enrolment

When the Cardholder initiates payment, the Merchant sends a Verify Enrolment Request (VEReq) message to the Visa Directory Server to determine whether the Cardholder's card is enrolled in VbV and must therefore be authenticated. The Visa Directory Server returns a Verify Enrolment Response (VERes) message.

31.6.2 Payer authentication

Upon receiving a VERes indicating that authentication is available, the Merchant sends a Payer Authentication Request (PAREq) message and forwards it to the Issuer ACS, whose URL was included in the VERes, via the Cardholder's browser. The Issuer ACS returns a Payer Authentication Response (PARes) message including the Issuer's authentication decision to the Merchant.

The possible outcomes of payment authentication and the codes used to communicate the Issuer's authentication decision are:

- Y for authentication successful
- N for authentication failed
- U for authentication could not be performed
- A for attempts processing performed

Upon receiving the PARes, the Merchant determines whether it is appropriate for the Merchant commerce server to submit an authorization request. See the Visa Europe processing specifications.

31.6.3 Authentication history

The ACS must send to the AHS a Payer Authentication Transaction Request (PATransReq) message, and receives a Payer Authentication Transaction Response (PATransRes) message from the AHS. This authentication activity is used by Visa Europe for dispute resolution and other purposes. Issuers and Acquirers have their own logs from the MPI (for Acquirer) or ACS (for Issuer) to respond to a dispute.

31.6.4 CAVV validation

When the Issuer or VEAS completes the CAVV validation process, it populates data subfield 44.13 - CAVV Results Code.

Acquirers include the CAVV and an Electronic Commerce Indicator (ECI) in DMSA 0100 authorization requests and in SMS 0200 full financial request messages.

Data Subfield 60.8 - Additional POS Information - Mail/Phone/Electronic Commerce and Payment Indicator contains the ECI value to submit in DMSA and SMS messages.

For more information and for a list of valid values for data subfields 44.13 and 60.8, see the Visa Europe technical specifications.

31.7 Key data fields

The following key data fields are used by the VbV Service. For detailed information, see the Visa Europe technical specifications.

Data field 22, Positions 1-2 - POS Entry Mode

The data source is the Merchant or the Acquirer. This data field must contain a value of 01 (key entry).

Data field 25 - POS Condition Code

The data source is the Merchant or the Acquirer. This data field must contain a value of 59 (VSEC request).

Data subfield 44.13 - CAVV Results Code

The data source is the Issuer or VEAS. This data field must contain the Issuer's response if the Issuer has completed CAVV validation.

Data subfield 60.8 - Additional POS Information - Mail/Phone/Electronic Commerce and Payment Indicator

The data source is the Merchant or the Acquirer. This data field must contain a value of 05, 06 or 07 (DMSA).

Data subfield 126.8 - Transaction Identifier (XID)

The data source is the Merchant. This data field must contain a unique number that the Merchant server generates to identify the transaction.

Data subfield 126.9, Usage 2 or 3 - 3-D Secure CAVV or 3-D Secure CAVV, Revised Format

The data source is the Merchant. This data field must contain the data value that the Issuer's ACS generated to enable VEAS or the Issuer to validate the CAVV results.

32 Visa Alternative Authorization Routing

Visa Alternative Authorization Routing (VAAR) enables Issuers to nominate an alternative Processor to process authorization requests on its behalf.

This service is invoked when the Issuer fails to respond in time or when the Issuer instructs Visa to send certain types of transaction requests to the alternative Processor.

The Issuer can opt for VAAR in addition to Visa's stand-in processing (STIP).

32.1 Related information

For further information please see the following documents:

- *Introducing the Visa Europe Authorization Service (VEAS)*
- *Introducing Stand-In Processing (STIP)*

32.2 Participation

Visa Alternative Authorization Routing is available to dual messaging Issuers.

32.2.1 Acquirer participation

Acquirers are not impacted by this service.

32.2.2 Issuer participation

Participation is optional for Issuers. Issuers that participate in the service need to specify a number of operating parameters.

The alternative Processor must be a Visa Europe Member.

The alternative Processor might hold data above and beyond that which Visa holds, for example, a card database or Cardholder available funds data.

It is the responsibility of the Issuer to synchronise Cardholder account data between the Issuer and the alternative Processor. Visa will provide the details of the response from the alternative Processor through an advice to the Issuer.

32.2.3 Planning and implementation

Issuers communicate details of the alternative Processor to Visa Europe by completing a *Member Information Questionnaire*. For more information, Members should contact Visa Europe Customer Support.

32.2.4 Testing and certification

Testing and certification depend upon the experience of the alternative Processor. A new Member will need to be fully certified for all aspects of transaction handling, while an existing Processor may only require certification for certain message types.

To ensure that Cardholders receive a consistent service, the alternative Processor should be certified at least to the same level as their associated Issuer.

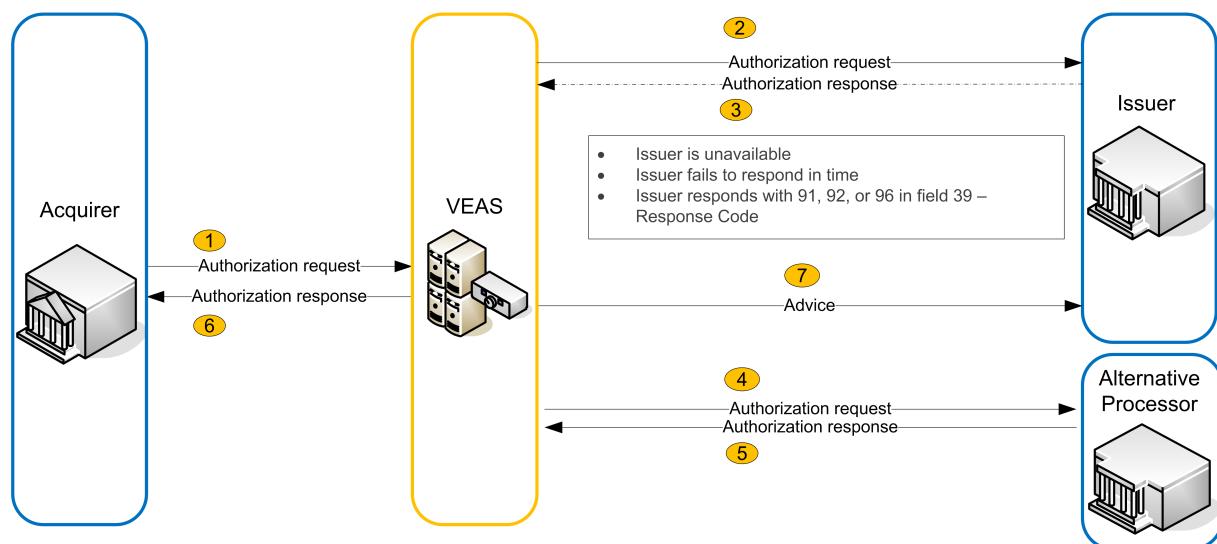
32.3 How the service works

The Visa Europe Authorization Service (VEAS) supports one alternative Processor for Issuers subscribed to the service. VEAS checks whether:

- The Issuer has opted in for Visa Alternative Authorization Routing
- Visa Alternative Authorization Routing can be invoked for the message type
- The Issuer has assigned an alternative Processor

32.4 Process flow

Figure 73: Visa Alternative Authorization Routing process flow



1. VEAS receives an authorization request from the Acquirer.
2. VEAS sends the authorization request to the Issuer.
3. VEAS sends the authorization request to the alternative Processor in the following circumstances:
 - a. The Issuer is unavailable
 - b. The Issuer fails to respond in time
 - c. The Issuer responds with response code 91, 92 or 96
4. The alternative Processor responds on the Issuer's behalf.
5. VEAS forwards the alternative Processor response to the Acquirer.
6. VEAS creates an advice for the Issuer informing them that the authorization request was processed by the alternative Processor. The Issuer obtains the advice in the same way as for STIP advices.

STIP may be invoked depending on set up and routing parameters. For example if the Issuer or alternative Processor responds with N0 (force STIP) in field 39, VEAS will respond on behalf of the Issuer or alternative Processor.

32.5 Key messages

For detailed information about the authorization messages used by Visa Alternative Authorization Routing, see the *DMSA Technical Specifications* manual.

Visa Alternative Authorization Routing can forward the following message types:

- 0100/0101 authorization request/repeat
- 0400/0401 reversal request/repeat
- 0120 Automated Fuel Dispenser (AFD) confirmation advices

Note 0120 AFD confirmation advices are forwarded only, they are not processed as authorization requests.

32.6 Key data fields

The following key data fields are used when Visa Alternative Authorization Routing is enabled.

Data field 39 – Response Code

The following response code values are applicable for all Issuers. However, if Visa receives any of these values from a VAAR-enabled Issuer, Visa routes the authorization request to the alternative Processor:

91 = Issuer unavailable

92 = Network routing not possible

96 = System malfunction

Data field 44.1 – Response Source/Reason Code

Acquirers are not impacted. The response code is the same whether the response is from the Issuer or the alternative Processor.

Data field 63.4 – STIP/Switch Reason Code

9021 = Indicates that the Issuer is unavailable and the transaction is diverted to an alternative Processor.

The STIP/Switch reason code is present only in the advice sent to the primary Issuer, to notify them of the alternative Processor decision.

33 Visa cash back Service

Visa cash back is a service which allows Cardholders access to cash at the point-of-sale (POS) when they make a purchase with their Visa card. It is a domestic service available on Visa cards, Visa Electron cards, and V PAY cards. It is a convenient way of withdrawing cash without the need to visit an ATM.

Members can participate by enrolling the appropriate Bank Identification Numbers (BINs) for the service. The service is optional for Issuers, Acquirers and their Merchants.

In all transactions involving cash back, the Merchant, the Acquirer, and the Issuer must operate in the same country.

Participation is by country, and each country must establish its own domestic parameters (that is, the maximum cash back amount limit).

The following table lists the cash back services supported by Visa Europe.

Table 44: Cash back services supported by Visa Europe

Cash back services supported by Visa Europe	Availability	Cards	Card type
Visa cash back Service	The Europe region (excluding UK)	Visa, Visa Electron, V PAY	Debit and credit
UK cash back Service	UK only	Visa, Visa Electron	Debit only

Note The range of cards and card types to which the Visa cash back Service may be offered is a domestic parameter and can vary between different countries.

33.1 Related information

For further information about the Visa cash back Service, see the following:

- *Visa cash back Guide*
- *Visa Europe Merchant Data Standards Manual*
- *Single Message System (SMS) POS Technical Specifications*
- *Dual Message System Authorization (DMSA) Technical Specifications*
- *Visa Smart Debit/Credit Personalization Assistant, Issuer User Guide EMV Integrated Circuit Card Specifications for Payment Systems*
- *Visa Integrated Circuit Card Specifications*

33.2 Participation

The Visa cash back Service is available through the dual and single messaging systems.

Participation is:

- Mandatory for Issuers of UK debit cards
- Optional for all other Members and Merchants

To participate in the service, Members must meet the following requirements.

Important The applicable payment scheme or processing rules allow the Visa cash back Service for Domestic Transactions only.

33.2.1 Standard and domestic operating parameters

The Visa cash back Service is governed by a series of mandated parameters. Certain parameters are standard and apply to all countries where the service is implemented, whilst others are set at the domestic level and can vary between countries. Members within a country must discuss and agree at board or executive committee level (or equivalent) an operating framework and approve the domestic parameters.

Table 45: Visa cash back Service - Standard and domestic operating parameters

Parameter	Type	Description
Domestic service only	Standard	Cardholder, Acquirer, Issuer must all operate in the same country.
Zero floor limit	Standard	All cash back transactions must be authorized online.
Must be in conjunction with a purchase	Standard	The Visa cash back Service can only be offered as an additional service to a purchase. It cannot be the complete transaction.
Cash back amount identified separately in a transaction	Standard	Cash back amount is mandated in field 61.1 - Other Amount, Transaction. This must be the sole use of this field.
Processed as a single purchase transaction	Standard	Purchase amount and cash back amount are routed as a single purchase transaction.
Interchange payable on purchase amount only	Standard	The Interchange Reimbursement Fee for the transaction is applied to the purchase amount only.
Standard Cardholder verification Method (CVM)	Domestic	It is recommended that the CVM for cash back transactions be consistent with existing point-of-sale (POS) transaction requirements.
Products	Domestic	Determine which cards the service may be used with. The service can be offered with Visa cards, Visa Electron cards and V PAY cards.
Cash back limit	Domestic	A maximum cash back limit sets a limit to the maximum amount that can be disbursed in a single transaction. The limit should be set to balance risk management and customer convenience.

Table 45: Visa cash back Service - Standard and domestic operating parameters (continued)

Parameter	Type	Description
Country-specific parameters		
United Kingdom only	Domestic	POS prompt enabled by the upload of the UK debit BIN range in the terminals.
Republic of Ireland only	Domestic	POS prompt enabled by the upload of the Irish debit BIN range in the terminals.

33.2.2 Issuer implementation considerations

Issuers choosing to participate in the service must:

- Be certified
- Consider how Cardholder daily cash limits will be affected by cash back
- Feature cash back transactions on Cardholder statements
- Review their Positive Cardholder Authorization Service (PCAS) parameters and adjust purchase limits as required to accommodate cash back amounts

STIP processing applies to the total Transaction Amount: it represents the Issuer's total exposure for the transaction. STIP does not consider the cash back amount separately.

33.2.2.1 Chip card considerations

Issuers should refer to the latest version of the *EMV Integrated Circuit Card Specifications for Payment Systems* and *Visa Integrated Circuit Card Specifications* (VIS) for details of the technical requirements at point-of-sale.

Issuers must ensure that their authorization systems can accept and process cash back data included in the authorization request cryptogram (ARQC).

Issuers need to evaluate the impact of cash back processing when determining personalisation settings. Personalisation considerations for cash back include:

- Cardholder Verification Method (CVM)
For purchase transactions with cash back, verification can be by PIN or signature, or restricted to PIN only.
 - Velocity checking by amount
Relates to the management of offline transactions. For velocity checking by amount, the amount relates to the transaction total (purchase **plus** cash back). When the accumulated amount of offline transactions exceeds the designated amount, the card triggers an online transaction.
 - Account usage control
'Domestic' cash back must be selected. Cards issued without this setting cannot be used to obtain cash back.
- Note** Cards may be issued with cash back enabled but not implemented, in anticipation of use at a future time.

33.2.3 Acquirer implementation considerations

Acquirers choosing to participate in the service must:

- Be certified
- Be able to format an authorization request with the total Transaction Amount (purchase **plus** cash back) in field 4- Amount, Transaction and the cash back amount in field 61.1 - Other Amount, Transaction
- Be able to receive and act on the following response and reject codes

Table 46: Response and reject codes

Code	Type	Meaning	Description
N3	Response	Visa cash back Service not available to the Cardholder	Indicates that the Issuer does not participate in Visa cash back.
N4	Response	Cash request exceeds Issuer limit	Indicates that the Cardholder has requested an amount: <ul style="list-style-type: none"> ■ Greater than the maximum cash limit for the country, or ■ Greater than the limit established between the Issuer and the Cardholder
0106	Reject	Invalid value	Indicates that the transaction was submitted for cash back only (no purchase amount). The cash back amount must be less than the total Transaction Amount.

33.2.3.1 Chip card transaction considerations

Chip card transactions must pass the cash back amount to the card when requested, and then pass the resulting cryptogram data from the card to the Acquirer for inclusion in the authorization message.

33.2.4 Testing and certification

Members participating in the service must consider the following:

- Certification is mandated in order to participate in the Visa cash back Service
- Members that do not complete certification will not be able to send transactions with cash back amounts
- Certification is at host level and includes both VEAS, and VECSS

Visa Member Testing Service (VMTS) provides testing and certification assistance. To arrange for testing and certification, Members should contact Visa Europe Customer Support.

33.2.5 Service monitoring

Information is collected on transactions going through the Visa Europe System, structured around the following parameters:

- Country
- Merchant Category Code (supermarkets, etc.)
- Card type (debit, credit)
- Number of POS transactions including cash back, split by debit/credit
- Value of POS transactions with cash back, split by debit/credit

Members must report their cash back volumes in terms of transaction volumes and transaction numbers in the quarterly Operating Certificates.

33.2.6 Planning and implementation

For more information, Members must contact Visa Europe Customer Support.

33.3 How the service works

Irrespective of the country in which the service operates, all Visa cash back transactions share certain common processing characteristics and requirements. Unless indicated otherwise, information in this section applies to all Visa cash back transactions.

Visa cash back transactions are supported in both dual and single message processing environments and are subject to standard Visa system edits.

The main steps in the Visa cash back Service are:

1. Merchant communicates cash back and full Transaction Amount to the Acquirer.
 - At the point-of-sale (POS), the Merchant may ask, or the terminal may prompt, the Cardholder if they require cash back
 - The cash back and purchase amounts are keyed separately
 - The POS device displays the total Transaction Amount and the Cardholder enters their PIN, or signs a receipt, to confirm the total amount
 - The Merchant's terminal sends the transaction details to the Acquirer; with the cash back amount identified separately, but as part of a single transaction
2. Acquirer creates an authorization request and sends it to VEAS.
 - The Acquirer receives the transaction data and creates an authorization request with the cash back amount identified in field 61.1 - Other Amount, Transaction, and for chip card transactions, additionally in field 55, tag 9F03 - Amount Other
3. VEAS performs edits and routes the authorization request to the Issuer.
 - VEAS performs the following checks. If a request fails any check, the authorization message is returned to the Acquirer; accompanied by the appropriate response or reject code

Table 47: Cash back fail conditions and corresponding processing rules

Fail condition	Processing rule	Response/reject code
Cardholder and Merchant are not in the same country.	Transaction declined.	N3 - cash back Service not available to Cardholder.
Issuer is not participating in Visa cash back.	Transaction declined.	N3 - cash back Service not available to Cardholder.
Acquirer is not participating in Visa cash back.	Transaction declined.	N3 - cash back Service not available to Cardholder.
Cardholder is trying to use a domestic cash back card in a different country, either in or outside the Europe region.	Transaction declined.	N3 - cash back Service not available to Cardholder.
The cash back amount is greater than the maximum cash back amount for the country.	Transaction declined.	N4 - cash back request exceeds Issuer limit.
The cash back amount is equal to the total Transaction Amount.	Transaction rejected.	0106 - invalid value.

- VEAS routes the message to the Issuer; to stand-in processing (STIP) if appropriate; to STIP if the Issuer is unavailable or fails to respond in time
4. Issuer approves or declines the transaction and sends an authorization response to VEAS.
- The Issuer considers the Cardholder's available funds and, where appropriate, daily cash limit
If the cash back amount is less than the maximum cash back amount for the country, but greater than the limit established between the Cardholder and the Issuer, where Members in a country agree, an Issuer could generate an authorization response indicating that the Merchant retry the transaction for a smaller cash back amount, or for the purchase amount only (response code must be N4).
 - The transaction is either approved or declined in its entirety - partial approval is not allowed
 - A transaction may be declined for a variety of reasons, including insufficient funds, or if the card has been reported as lost or stolen
5. VEAS routes the Issuer's response to the Acquirer.
6. Acquirer responds to the Merchant.
- If the transaction is approved, the Merchant's terminal generates a customer receipt showing the cash back amount identified separately. Merchant sells the goods and disburses cash to the Cardholder
 - If the transaction is declined, no cash is disbursed to the Cardholder
7. The transaction is cleared and settled.

33.3.1 Stand-in processing

When an Issuer is not available, or when determined by Positive Cardholder Authorization Service (PCAS) settings, VEAS progresses the request using stand-in processing (STIP).

STIP processing applies to the total Transaction Amount: it does not consider the cash back amount separately. If STIP authorizes the transaction on the Issuer's behalf, it generates an authorization response and sends it to the Acquirer without routing the transaction to the Issuer. Depending on the STIP options set by the Issuer, an advice may be created to inform the Issuer of the STIP decision.

Maximum cash back limits for participating countries are maintained by Visa Europe.

33.3.2 Exception processing - chargebacks

For Visa cash back transactions, chargebacks are valid for the purchase amount or for the total Transaction Amount.

The purchase amount, full or partial, can be charged back for a valid reason, such as damaged goods.

The cash back amount cannot be charged back by itself. The cash back amount can only be charged back when the entire transaction, including the full purchase amount, is being disputed.

33.3.3 Chip card data

Acquirers submit chip data in field 55 (tag-length-value format). However, Issuers may opt to receive such data in the third bitmap, fields 147 and 149. When required, VEAS ensures that the data is transmitted and received in the appropriate fields.

33.3.4 UK cash back Service

The UK cash back Service can be used with Visa cards and Visa Electron cards. VEAS processes UK cash back requests as dual message transactions. The 0100 authorization requests must include a valid Merchant Category Code (MCC).

In the UK, terminals at **all** points-of-sale, where the service is offered, hold a separate table of Visa UK debit BIN ranges. This facilitates prompting for the service.

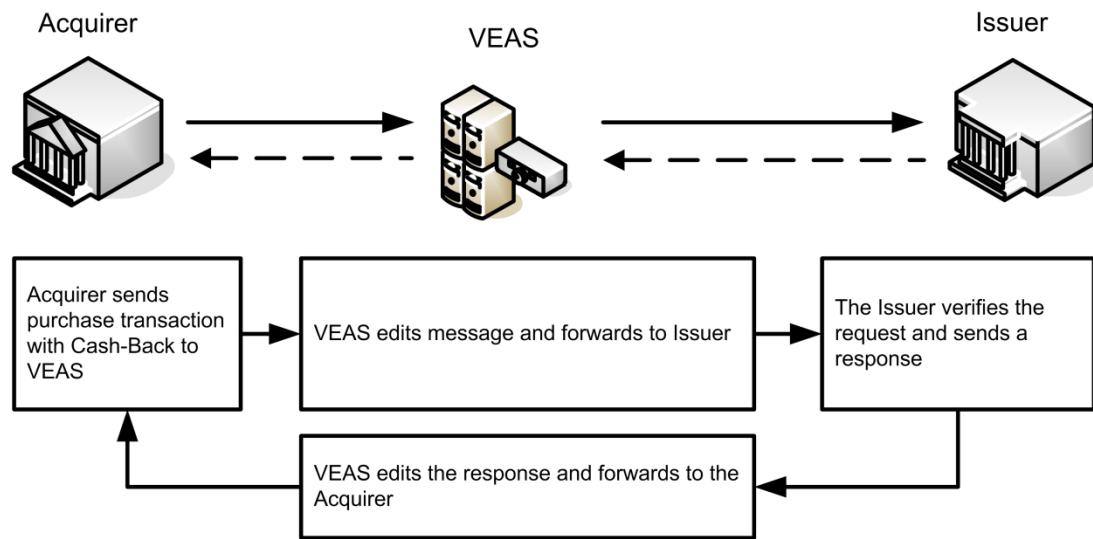
If the Merchant, the Acquirer, and the Issuer are not all operating in the UK, VEAS may decline the transaction with response code 57 - Transaction Not Permitted.

For maximum cash back amounts and for other country-specific information, Members should contact Visa Europe Customer Support.

33.4 Process flow

The following diagram illustrates the process flow for the Visa cash back Service.

Figure 74: Process flow for the Visa cash back Service

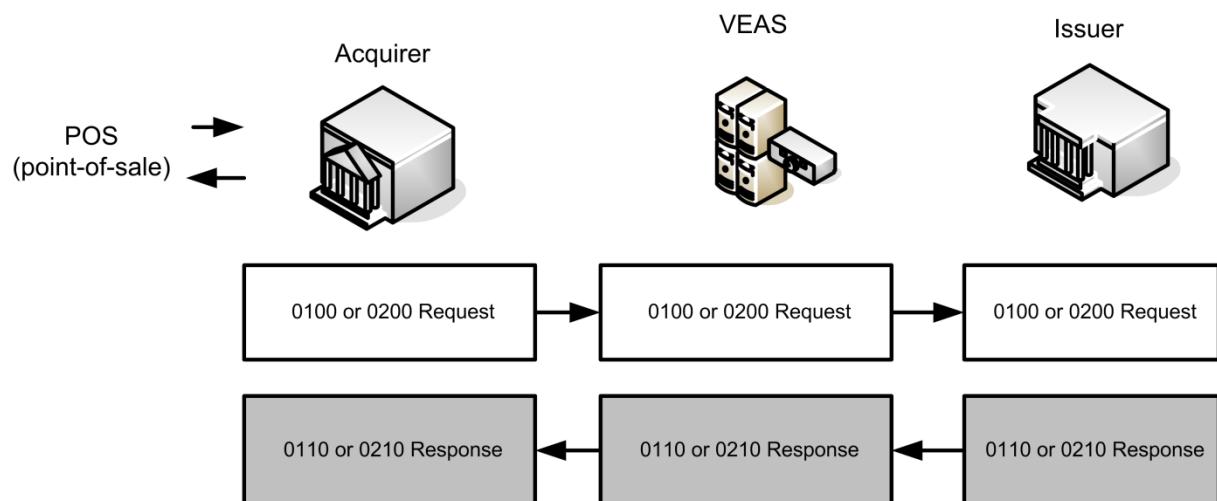


1. An authorization request including cash back is raised by the Acquirer and sent to the Issuer.
2. Issuer responds to Acquirer.

33.5 Message flow

The following diagram illustrates the message flow for the Visa cash back Service.

Figure 75: Message flow for the Visa cash back Service



1. Merchant terminal generates a purchase request with cash back.
2. Acquirer sends a 0100 or 0200 request with cash back to VEAS.
3. VEAS edits the message, and forwards to the Issuer.
4. Issuer verifies the request and sends a 0110 or 0210 response to VEAS.
5. VEAS forwards the response to the Acquirer.

6. Acquirer responds to Merchant.
7. Merchant terminal processes the request and generates a receipt showing the cash back amount.
8. Transaction is cleared and settled.

33.6 Key messages

The following messages carry the Visa cash back Service:

- 0100 authorization request
- 0110 authorization response
- 0200 financial transaction request
- 0210 financial transaction response

33.7 Key data fields

The following key data fields are used by the Visa cash back Service. For detailed information, see the Visa Europe technical specifications.

Data field 4 - Amount, Transaction

This data field contains the total Transaction Amount. For a transaction that includes cash back, this is the purchase amount **plus** the cash back amount in field 61.1.

Data field 43 - Card Acceptor Name/Location

This data field identifies the Merchant's country and name.

Data field 55 - VSDC Chip Data

Data field 55 is mandated for use by Acquirers. The following two tags are used:

- 9F02 - amount authorized (maps to field 147)
 - Used by the chip when calculating the cryptogram.
 - For a transaction that includes cash back, this is the total of the purchase amount **plus** the cash back amount.
- 9F03 - amount, other (maps to field 149)
 - Used by the chip when calculating the cryptogram.
 - If the transaction involves cash back, this field must be present and be included in the authorization request cryptogram (ARQC) algorithm.
 - If the transaction does not involve cash back, this field may be present and the ARQC may be calculated with a zero cash back amount.

Data field 61.1 - Other Amount, Transaction

This data field contains the cash back amount. The amount in this field must be less than the amount in field 4.

Data field 147 - Cryptogram Amount

If an Issuer processes the third bitmap, this field contains the Transaction Amount.

Data field 149 - Cryptogram Cash Back Amount

If an Issuer processes the third bitmap, this field contains the cash back amount.

34 Visa Device Profiling

Visa Device Profiling (VDP) is a fraud management service that monitors cross-border activity originating from ATM devices where the chip has not been read. The service uses a series of behavioural algorithms to analyse an ATM's daily activity and predict the likelihood of fraudulent cash withdrawals occurring over the next 24 hours.

This service is designed for both Issuers and Acquirers:

- **VDP for Issuers**
Provides Issuers with a daily overview of unusual cross-border ATM Transaction patterns and trends, as well as details of any of their transactions that have taken place at suspect ATMs.
- **VDP for Acquirers**
Provides Acquirers with a daily overview of unusual cross-border ATM Transaction patterns and trends, as well as details of any suspect activities taking place at their own ATMs.

Members who are both Issuers and Acquirers have access to both sets of functions.

34.1 Related information

The following documents contain further information about VDP:

- *Visa Device Profiling Member Implementation Guide*
- *Visa Device Profiling for ATMs User Guide for Issuers and Acquirers*
- *Visa Device Profiling Fraud Solution Frequently Asked Questions (FAQs)*

34.2 Participation

Participation in VDP is optional for Members.

Members that choose to participate in the service must have an active Visa Online (VOL) subscription.

34.2.1 Planning and implementation

No system changes or technical implementation measures are needed. Members access the service through their existing VOL subscription.

34.3 How the service works

This section gives a high-level overview of how the VDP service works.

1. A Member's VOL Access Manager uses the VOL Access Manager application to request access for users to the VDP application.
2. Visa Europe activates the Member's subscription.
Authorised users and administrators can now access the VDP application.

3. Member accesses reports on a daily basis.

Overnight, the previous 24 hours of authorizations traffic is filtered to leave only cross-border ATM Transactions where a chip has not been read. For each unique ATM that has processed a cross-border transaction, the following processing happens:

- The ATM usage is rated using 22 different criteria to produce a score ranging from zero (unremarkable) to 1000 (very high likelihood of fraud attack in the next 24 hours).
- The scores are graded by severity into one of four colour codes as to their current susceptibility for fraud.

Each user will receive Member-specific interactive reports and associated data on a daily basis.

34.3.1 Subscription and access rights

When Members subscribe to VDP they request access for one or more users. There are two types of access rights for the service:

- User

Can access the VDP strategic and operational reports. For more information, see [Reports delivered by VDP](#) below.

- Administrator

Administrators have all privileges of users. In addition, they can change users' access to reports, and create and amend report templates.

Report templates enable the Member to control what information is made available to its users. Once created, the administrator can assign an appropriate user to that report template. For more information, see the *Visa Device Profiling for ATMs User Guide for Issuers and Acquirers guide*.

Note Members must appoint at least one administrator.

34.4 Reports delivered by VDP

The VDP service delivers two types of reports:

- Strategic reports
- Operational reports

34.4.1 Strategic reports

Strategic reports are a suite of reports refreshed daily, that supply a set of predefined views, showing the potential fraudulent exposure at ATM devices identified as suspect in the previous 24 hours and likely to be attacked in the following 24 hours. Users can configure the views to determine trends over time and filter the information to view a subset of the data.

There are three types of strategic reports:

- Dashboard reports
 - Provides an executive summary snapshot, showing a graphical overview of potential ATM attacks. It provides a quick entry point to data from specific regions', countries' or cities'.
- Global Top Ten reports
 - Provides detailed information on specific ATMs with the highest predictive scores.
- Suspect ATM
 - Provides graphical and tabular information on potential cross-border ATM exposure at global, regional, country, city or ATM device levels. Members can generate reports for a single day or over a period of days or months.

Members can export strategic reports to a comma-separated values (CSV) file, suitable for loading into a spreadsheet program.

For detailed information about strategic reports, see the *Visa Device Profiling for ATMs User Guide for Issuers and Acquirers* guide.

34.4.2 Operational reports

The type of operational report that a Member receives depends on whether they are logged on as an Issuer or an Acquirer:

- Issuers receive the following operational reports:
 - ATM Issuer reports
 - Contains a list of all the ATMs from the previous 24 hours that have been marked as suspect, including devices where the Issuer's cards have not been used.
 - Authorization Transaction reports
 - Contains details of the Issuer's transactions that have taken place at an ATM identified as suspect.
- Acquirers receive ATM Acquirer reports. These contain details of the Acquirer's ATMs that have been identified as suspect.

For detailed information about operational reports, see the *Visa Device Profiling for ATMs User Guide for Issuers and Acquirers* guide.

35 Visa Europe Payment Stop Service

The Visa Europe Payment Stop Service (payment stop service) enables Issuers, on instruction from a Cardholder, to place a payment stop instruction against an authorization request or a clearing record for a recurring transaction or an instalment transaction:

- Recurring transactions are a series of transactions processed following agreement between a Cardholder and a Merchant where the Cardholder purchases goods or services over a period of time through a number of separate transactions
- Instalment transactions represent a single purchase of goods or services billed to a Cardholder's account in multiple segments, over a period of time that has been agreed between the Cardholder and a Merchant

When an Issuer creates a payment stop instruction through the service, the Visa Europe System initiates the following series of events when they find a match:

- In the Visa Europe Authorization Service (VEAS), declines any matching authorization requests
- In the Visa Europe Clearing and Settlement Service (VECSS), returns any matching Clearing records initiated within the Europe region
- Where requested, and where possible, updates the Visa Account Updater (VAU) file with details of the payment stop instruction

As well as creating payment stop instructions, Issuers can use the payment stop service to amend or cancel existing payment stop instructions and view high-level reports.

35.1 Related information

For further information relating to the payment stop service, see the following documents:

- *Visa Europe Payment Stop Service User Guide*
- *Visa Europe Merchant Data Standards Manual*
- *Visa Europe Fee Guide*
- *Visa Europe Visa Account Updater Service Member Implementation Guide*

35.2 Participation

The payment stop service is implemented in the Visa Europe System and uses existing codes. Participating Members access the service through VOL. As a result, there are no additional technical requirements to access the service.

Participation is optional for Issuers.

Members do not need to make changes to their host systems. However, there are some impact considerations for Acquirers and Issuers.

35.2.1 Impact considerations for Acquirers

Acquirers do not need to subscribe to the service and no changes to their host systems are required.

For transactions that have been stopped by Issuers through the service, Acquirers must advise their Merchants that:

- Authorization requests will be declined with existing response codes R1 and R3
- Authorizations declined using response codes R1 or R3 must not be re-submitted
- Clearing messages will be returned using existing return reason codes C1 and C2

Acquirers may continue to check VAU for active payment stop instructions as VAU should be updated when a payment stop instruction is created, amended or cancelled in the payment stop service if the Merchant is registered in that service.

For more information, see the *Visa Europe Payment Stop Service User Guide*.

35.2.2 Impact considerations for Issuers

No changes to Issuer host systems are required when subscribing to the payment stop service. However, Issuers should note the following and modify their processes accordingly:

- Issuers must create payment stop instructions through the payment stop service, not VAU, in order for stopped transactions to be automatically declined or returned to the Acquirer.
The payment stop service will pass payment stop instruction information to VAU to notify Acquirers and Merchants in advance that a payment stop instruction is in place. However, payment stop instruction information sent directly to VAU by the Issuer will not be passed back to the payment stop service to be processed.
Therefore, Issuers subscribing to the payment stop service should discontinue sending payment stop instruction information directly to VAU (including Issuers that accumulate and send updates in batch files to VAU).
- Issuers will receive an advice each time a transaction is stopped in VEAS by the payment stop service. Within these advices, Issuers will see codes that they have not previously received in advices. These are existing decline response codes R1 and R3 and Issuers are advised to check that these can be correctly handled.
- All Stand-In Processing (STIP) services apply even if the transaction is stopped in VEAS by the payment stop service. This means that the R1 or R3 decline response codes will be replaced if a higher priority STIP response code applies.

For more information, see the *Visa Europe Payment Stop Service User Guide*.

35.2.3 Planning and implementation

For more information, Members must contact Visa Europe Customer Support.

35.3 How the service works

A Cardholder requests a recurring or instalment payment be stopped. Their Issuer accesses the payment stop service through VOL and checks the eligibility of the request and whether a payment stop instruction already exists. If the request meets the eligibility criteria, the Issuer creates the payment stop instruction to stop the payment being authorized and/or cleared.

The payment stop service:

- Enforces the payment stop instruction from the next calendar day (default) or a future start date specified by the Issuer
- For participating Issuers, sends details of the newly created, amended or cancelled payment stop instruction to VAU

35.3.1 Levels of payment stop instructions

There are three levels of payment stop instructions:

- PAN level
A Cardholder wishes to stop all future recurring transactions and instalment transactions on their Personal Account Number (PAN).
- MCC level
A Cardholder wishes to stop all future recurring transactions and instalment transactions on their PAN, against a specific Merchant Category Code (MCC).
- Merchant level
A Cardholder wishes to stop all future recurring transactions and instalment transactions to a specific Merchant. The Cardholder can specify amount and date ranges to stop a single payment where multiple payments occur each month with the same merchant.

35.3.2 Transaction eligibility

Prior to entering VEPSS, all transactions are pre-screened to determine their eligibility for the payment stop service. The detailed rules for transaction eligibility are confidential.

Transactions determined as eligible are then checked by VEPSS and stopped if a match is found with an active stop instruction.

35.3.3 Interaction with other services

Whenever an Issuer creates or amends a payment stop instruction in the payment stop service, it is communicated to VEAS, VECSS and, for participating Issuers, VAU:

- VEAS
When an authorization request for an eligible transaction is received by VEAS and it matches an active payment stop instruction, the authorization request is declined and an advice is sent to the Issuer.

- VECSS

When a clearing record for an eligible transaction is received by VECSS, and it matches an active payment stop instruction, the clearing record is returned but an advice is not sent to the Issuer.

Important Clearing records from non-Visa Europe Acquirers processed through BASE II cannot be returned by VECSS under any circumstances even if a matching payment stop instruction is in place.

- VAU

Issuers that subscribe to VAU can instruct the payment stop service to send details of newly created and amended payment stop instructions to VAU. VAU does not automate the enforcement of payment stop instructions. Acquirers and registered Merchants can use the information available in VAU to look for payment stop instructions and prevent transactions from being submitted.

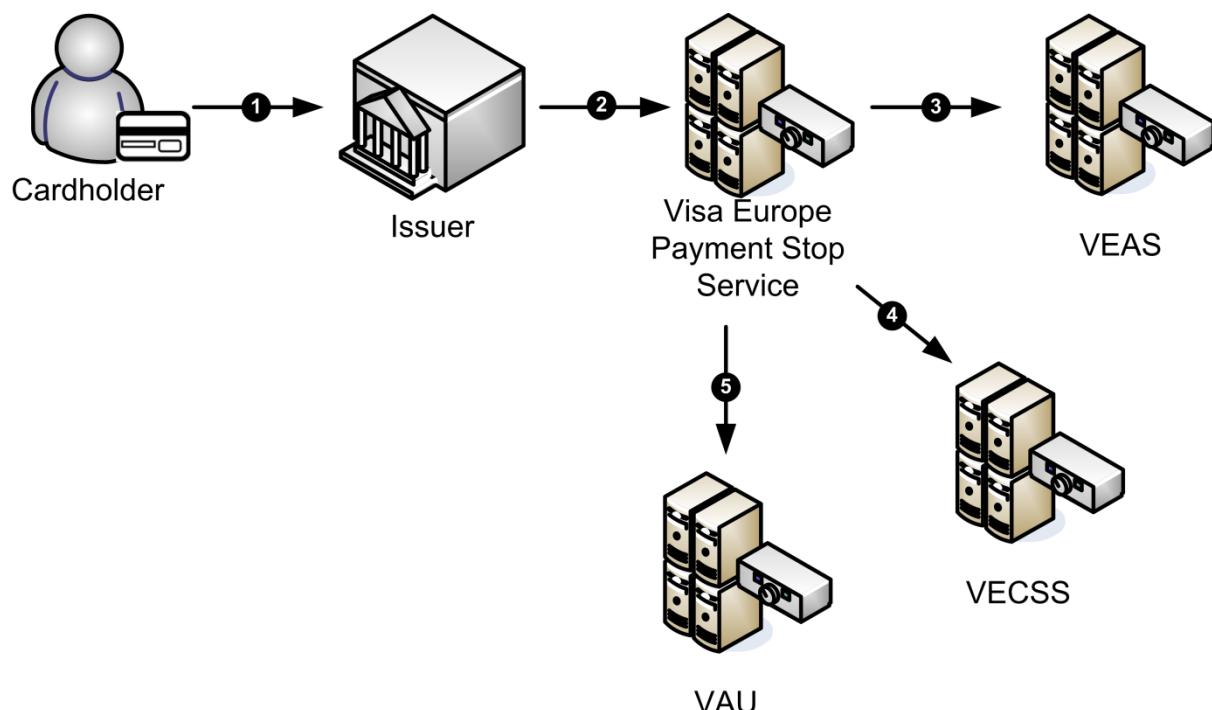
For more information on VAU, see the *Visa Europe Visa Account Updater Service Member Implementation Guide*.

For more information on how the payment stop service interacts with VEAS, VECSS and VAU, see the *Visa Europe Payment Stop Service User Guide*.

35.4 Process flow

The process flow between the payment stop service, VEAS, VECSS and VAU is described in this section.

Figure 76: Process flow for the payment stop service



1. Cardholder instructs their Issuer to stop a recurring or instalment payment.
2. Issuer creates a payment stop instruction in the payment stop service to stop an eligible payment from being authorized and/or cleared.
3. The payment stop service enforces the payment stop instruction in VEAS from the next calendar day (default) or a future date specified by the Issuer.

When a stopped transaction is subsequently received for Authorization:

- VEAS declines the transaction and sends an authorization response to the Acquirer
- Issuer is advised the authorization request has been declined

4. The payment stop service enforces the Clearing stop instruction in VECSS from the next calendar day (default) or a future date specified by the Issuer.

When a stopped transaction is subsequently received for Clearing, VECSS returns the Clearing record on behalf of the Issuer with a return reason code.

5. On the instruction of Issuers that subscribe to VAU, the payment stop service sends information about payment stop instructions to VAU.

When a participating Merchant subsequently requests a card update from their Acquirer:

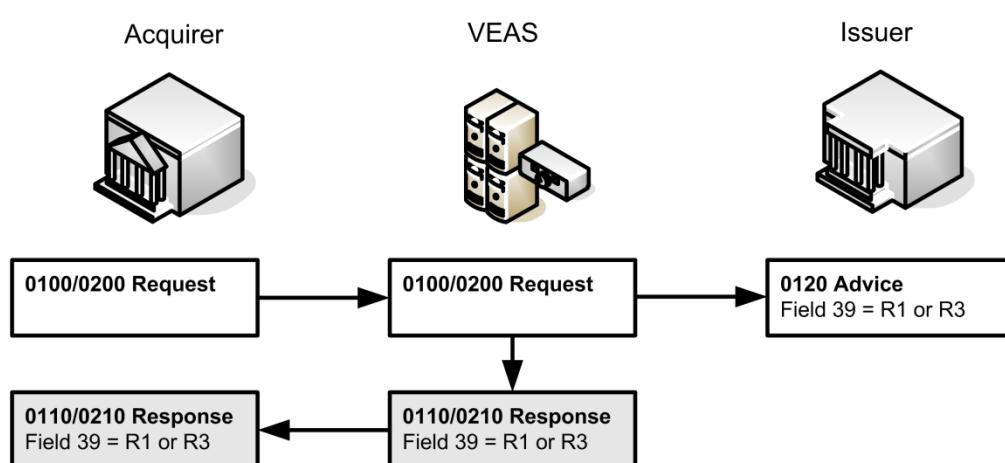
- Acquirer checks VAU for the latest card details and payment stop instructions
- Acquirer updates the Merchant

For more information, see the *Visa Europe Payment Stop Service User Guide*.

35.5 Message flows

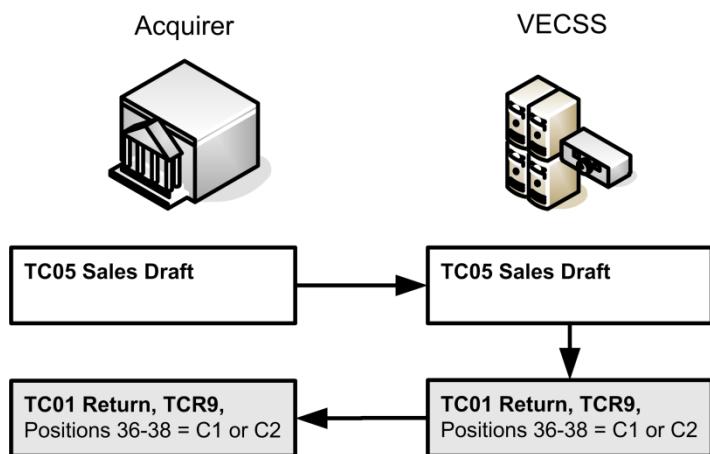
The following diagram illustrates the message flow for an authorization request declined by the payment stop service.

Figure 77: Message flow for an authorization request declined by the payment stop service



The following diagram illustrates the message flow for a Clearing record returned by the payment stop service.

Figure 78: Message flow for a Clearing record returned by the payment stop service



35.6 Key messages

35.6.1 Authorization

The following are the key messages for the payment stop service:

- 0100 authorization request
- 0110 authorization response
- 0120 authorization advice
- 0200 full financial request
- 0210 full financial response

35.6.2 Clearing

The following are the key Clearing records for the payment stop service:

- TC 01, Returned item transactions
- TC 05, Draft data transactions

35.7 Key data fields

The following key data fields are used by the payment stop service to determine transaction eligibility for VEPSS. For detailed information, see the Visa Europe technical specifications.

35.7.1 Authorization

The following are the key Authorization data fields for the payment stop service.

Data field 22 - POS Entry Mode Code

This data field contains a code indicating the method used to enter the Account and card expiry date into VEAS and, if an electronic terminal is used, the capability of terminal to capture PINs.

Data field 25 - POS Condition Code

This data field contains a code identifying transaction conditions at the point-of-sale or point of service.

Data field 39 - Response Code

This data field contains a code identifying the response to an authorization request.

Data field 60.8 - ECI/MOTO Indicator

This is the mail/phone/electronic commerce and payment indicator.

Data field 126.13 - POS Environment Code

This data field may contain an indicator for either recurring or instalment payments.

35.7.2 Clearing

The following is the key Clearing data field for the payment stop service.

TC 01 TCR 9 - Return Reason Code

The code will be set to one of the following values:

- C1 - Revocation of Authorization
MCC or Merchant level payment stop requests
- C2 - Revocation of all authorizations order
PAN level payment stop requests

36 Visa Member Testing Service for VEAS

The Visa Member Testing Service (VMTS) for the Visa Europe Authorization Service (VEAS) enables Members and their Processors to test their message formats and authorization interfaces with VEAS.

VMTS helps Members to test their parameter configurations, message formats and Visa Europe System data transmission. It enables Members to identify and fix potential problems before new or enhanced Visa Products and Services are activated. In many cases, parameters such as those used for test BINs can then be transferred to the production system.

VMTS for VEAS supports testing by simulating the VEAS, but in a physically separate environment. It supports end-to-end testing of authorization by performing the role of an Acquirer or an Issuer, depending on the role being tested.

The purpose of testing using VMTS for VEAS is to:

- Verify that the components of new participating systems, or existing systems that have been enhanced or changed, can communicate accurately with the Visa Europe System.
- Provide a test environment for new Members and Processors, and for existing Members and Processors when modifying their set ups.
- Enable Visa Europe staff to investigate negative test results.
- Enable Members to obtain VisaNet certification, where Visa Europe performs specific tests with Members and verifies the results. VisaNet certification reduces the possibility that problems will occur in production.

Important If the Member chooses to test their authorization system with Visa Europe, they must use VMTS for VEAS.

36.1 Visa Member Testing Service for VEAS and production differences

VMTS does not completely replicate the production environment. A number of services are either not supported or operate differently. For information on the testing provided by VMTS for specific services, Members must contact Visa Europe Customer Support.

36.2 Related information

For further information about the Visa Member Testing Service for VEAS, see the following:

- *VisaNet Certification Management Service Testing Guide - V.I.P., Member Version*
- *Visa Test System - V.I.P. User's Guide*
- Member Implementation Guide (MIG) for the service being tested

36.3 Participation

The Visa Member Testing Service for VEAS is available to Members and their Processors that use the VEAS production environment.

Participation is optional for Members and their Processors.

Members must retest when they:

- Activate a new service or enhance an existing service
- Install new, or modify existing, host system hardware or software
- Install hardware and software after a business enhancements release

Important All testing must be conducted using the VMTS test environment.

Only test account numbers and test keys must be used.

Acquirers must use the Visa Europe test BINs and account numbers provided by their Visa Europe Implementation Consultant.

36.3.1 Planning and implementation

To initiate a testing project, Members must raise a project; contact Visa Europe Customer Support.

Visa Europe Service Implementation Consultants and Technical Implementation Consultants (TIC) coordinate and validate Member testing. Their tasks include:

- Setting up the system parameters to reflect requirements
- Supporting provision and creation of Member test data where required
- Reviewing authorization requests to verify successful testing

In addition to working with their Visa Europe Technical Implementation Consultant, Members can also obtain instructions for new services and business enhancements (biannual releases) from the *VisaNet Business Enhancements Member Implementation Guide* for each service. This guide lists the transaction type requirements that must be processed through VMTS for VEAS to meet the specified success criteria.

36.3.1.1 Testing strategy

Visa Europe strongly recommends that Members use the VMTS to complete the following phases of testing:

- **Preparation and setup**

Visa Europe Service Implementation Consultants work with participating Members to collect information, schedule testing and assist when necessary.

- **Testing**

Visa Europe Technical Implementation Consultants assist participating Members to perform testing.

- **Validation** (optional)

Visa Europe Technical Implementation Consultants assist in validating that the participants' systems can interact with Visa Europe in an authorization environment for both incoming and outgoing messages.

Note Validation may not be carried out in all test scenarios. The scope of the testing must be discussed and decided when defining the requirements of the project.

36.3.1.2 Components required

Members need the following components to perform testing using VMTS:

- VMTS connectivity.
- Extended Access Server (EA Server).
- Accounts for testing - When testing a Member host that is acting as an Acquirer, Visa Europe provides the accounts or physical test cards for testing. When testing the Member host acting as an Issuer, the Member provides the accounts or physical cards for testing to the Visa Europe Implementation Consultant.

To facilitate testing, Visa Europe recommends that Members establish a method to run a test system comprising their hardware and software and a methodology to verify that the test transactions are updating their systems as expected.

36.3.1.3 VMTS constraints

Capacity in VMTS is limited. Volume or stress testing is not available.

VMTS is unavailable twice each year, during March and September, for a week each time. This downtime is scheduled for business enhancements. If any other downtime is scheduled, Members will be notified.

36.3.1.4 Member tasks

The principal member tasks are:

- Creating authorization test data
Depending on the role of the Member being tested (Acquirer or Issuer), the Member is expected to initiate a transaction with a message, and respond to various types of message received from VMTS. The Member must create the test data required for these messages.
- Sending test messages
Based on the tests required, Members might be asked to send different types of authorization message; for example, an authorization request for an ATM Transaction, or a balance inquiry.

For information on the testing tasks for new services or business enhancements, see the *VisaNet Business Enhancements Member Implementation Guide* for each service.

36.3.1.5 Success criteria

Participants must be able to send and receive authorization message formats and new data elements for new services or business enhancements. For more information on the success criteria for new services or business enhancements, see your Technical Implementation Consultant.

If an authorization message sent by a Member is rejected by VMTS, refer to the Visa Europe technical specifications to fix the problem and resubmit the test. Otherwise testing may be regarded as unsuccessful.

There are several authorization certification services available for Members. For example:

- ATM certification
 - Available within all countries of the Europe region, this includes certification for cash disbursements and, optionally, balance inquiries.
- Visa cash back certification
 - This is only available within some countries of the Europe region.

For information about all the available certification services and how to request them, contact your Visa Europe Implementation Consultant.

36.4 How the service works

VMTS simulates VEAS. It tests the Member's host system by simulating the other components involved in the authorization process, such as the other Member's host system and VEAS, and by testing the messages that are passed between them.

The Member host is connected to an Extended Access Server (EA Server) that, in turn, is connected to VMTS through a network. A VTS3 test station is also attached to the EA Server and can assume the opposing role to the Member role being tested, that is, act as the Issuer when testing the Acquirer role, and vice versa.

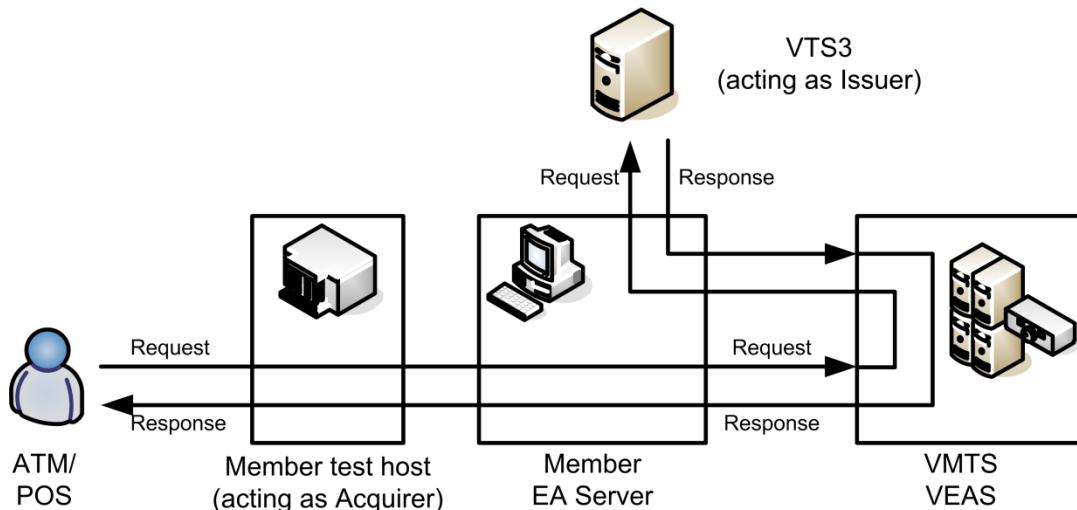
This configuration is known as VisaNet Loopback. It uses a network connection between the EA Server and VMTS in a test environment to closely replicate the VEAS production environment.

Members can test their systems themselves (Member self-testing) or with the help of a Visa Europe Technical Implementation Consultant. These methods are described below.

36.4.1 Member self-testing

The Member uses their test host and VTS3 to perform self-testing. Depending on the Member's role being tested, the test host sends and receives messages through an EA Server to the VMTS and the VTS3 (and, when testing the Acquirer role, from and to an ATM and/or point-of-transaction terminal).

The example in the following diagram shows the configuration required for the Member to test the Acquirer role.

Figure 79: Using VMTS to test the Acquirer role

In this example, the transaction is initiated from an ATM and/or Point-of-Transaction terminal with a request (for example, an authorization request or a balance inquiry). The request passes through the Member's test acquiring host to the Member's EA Server, which routes it to VMTS.

Because this is VisaNet loopback mode, the request is then routed back to the Member's EA Server which routes it on to the VTS3 acting as the Issuer. The response (for example, an authorization response) returns along the reverse route.

For Member self-testing, the Member must set up the VTS3 database to send and respond to messages. Member self-testing can be carried out without the assistance of a Visa Europe Technical Implementation Consultant.

36.4.2 Testing with a Technical Implementation Consultant

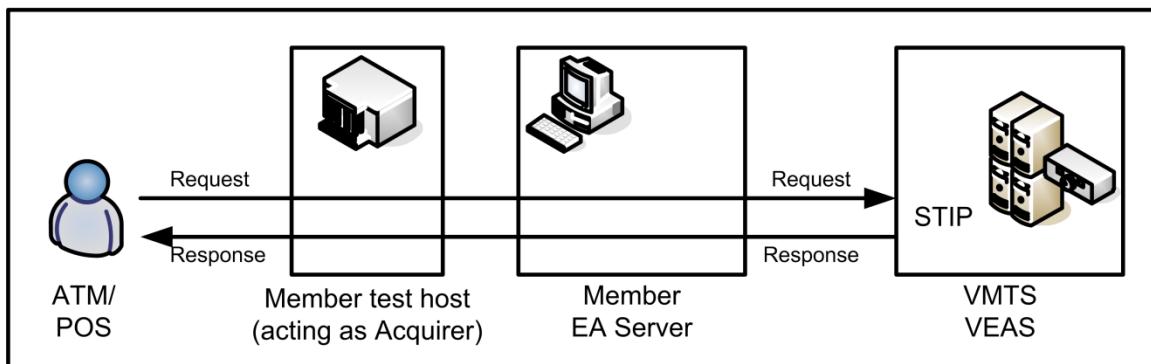
The configuration is similar to that for Member self-testing except that, instead of setting up their own VTS3 database, the Member has the option of using VMTS stand-in processing (STIP) and/or the Visa Europe Technical Implementation Consultant's VTS3 (or equivalent test tool) to perform the testing and certification.

36.4.2.1 Testing using the Technical Implementation Consultant's VTS3

When testing with the Technical Implementation Consultant's VTS3, the routing of messages is the same as for Member self-testing. In this case however, the TIC sets up the VTS3 database to send and respond to messages rather than the Member's VTS3.

36.4.2.2 Testing using STIP

When testing using VMTS to provide a STIP response, no VTS3 is required. The example in the following diagram shows the configuration required for the Member to test the Acquirer role using STIP.

Figure 80: Using VMTS to provide a STIP response

In this example, the transaction is initiated from an ATM and/or point-of-transaction terminal. The request passes through the Member's test acquiring host to the Member's VEAS, which routes it to VMTS. The VMTS STIP provides the response, which returns along the reverse route.

36.4.3 Message testing

VMTS simulates the Visa Europe Authorization Service by responding to request messages sent by the Member's host. It also sends requests to the Member's VEAS to test the Member's ability to route the message to their host and to send the correct response messages.

When a message is received from the host being tested, VMTS validates the field contents within the message, for example field length, field type (binary, hexadecimal, bits, and so on), minimum and maximum values, table lookups, the presence of mandatory fields in a message, and some checking of contents against the contents of related messages.

37 Visa Member Testing Service for VECSS

The Visa Member Testing Service (VMTS) for the Visa Europe Clearing and Settlement Service (VECSS) enables Member and Processor staff to test message formats and clearing and settlement interfaces with VECSS.

VMTS helps Members to test their VECSS parameter configurations, transaction formats, report formats and Visa Europe System data transmission. It helps Members to identify and fix potential problems before new or enhanced Visa Products and Services are activated.

It provides Members' testing staff with a dedicated environment for testing their systems with Visa Europe. Participants in VMTS can verify that their transaction formats, and offline clearing and settlement interfaces are working correctly before connecting to the Visa Europe System in a production environment.

VMTS supports testing by simulating the Visa Europe production systems, but in a physically separate environment. VMTS ensures that messages pass format and edit checks.

The purpose of testing using VMTS for VECSS is to:

- Verify that the components of participating systems that have been enhanced or changed can communicate accurately with the Visa Europe System
- Provide an environment for new Members or modification of existing Member setups, Processing Endpoints and new services or products
- Enable Visa Europe staff to investigate negative test results

37.1 Visa Member Testing Service for VECSS and production differences

VMTS does not completely replicate the VECSS production environment. A number of services are either not supported or operate differently. For information on the testing provided by VMTS for specific services, Members must contact Visa Europe Customer Support.

37.2 Related information

For further information about the Visa Member Testing Service for VECSS, see the following:

- *VisaNet Certification Management Service Testing and Certification Guide - BASE II Clearing, Member Version*
- *VisaNet Certification Management Service User's Manual - BASE II Clearing*
- Member Implementation Guide (MIG) for the service being tested

37.3 Participation

VMTS for VECSS is available to Visa Europe Members and their Processors that use the VECSS production environment.

Participation is optional for Members and their Processors.

Members must retest when they:

- Activate a new service or enhance an existing service
- Install new, or modify existing, host system hardware or software
- Install hardware and software after a business enhancements release

Important All testing must be conducted using the VMTS test environment.

Only test account numbers must be used.

Acquirers must use the Visa Europe test BINs and account numbers provided by their Visa Europe Implementation Consultant.

37.3.1 Planning and implementation

Visa Europe Service Implementation Consultants and Technical Implementation Consultants coordinate and validate Member testing. Their tasks include:

- Setting up the system parameters to reflect requirements
VMTS for VECSS can provide Customized File Delivery Type (CFDT) that allows Processing Endpoints to request various kinds of customised delivery files. This functionality can be used in VMTS to separate transactions originated by responder BINs from those originated by non-responder BINs.
To request a CFDT for transactions originated by responder BINs, Members must contact Visa Europe Customer Support.
Note CFDT is only available for delivery files.
- Supporting creation of Member test data
- Reviewing VECSS and Edit Package reports to verify successful testing

In addition to working with their Visa Europe Technical Implementation Consultant, Members can also obtain instructions for new services and business enhancements (biannual releases) from the *VisaNet Business Enhancements Member Implementation Guide* for each service. This guide lists the transaction type requirements that must be processed through VMTS for VECSS to meet the specified success criteria.

Note Before beginning testing, Members must tell their Technical Implementation Consultants which responder BINs they want to activate.

37.3.1.1 Testing strategy

Visa Europe strongly recommends that Members use the VMTS to complete the following phases of testing:

- **Preparation and setup**

Visa Europe Service Implementation Consultants work with participating Members to collect information, schedule testing and assist when necessary.

- **Testing**

Visa Europe Technical Implementation Consultants assist participating Members to perform testing.

- **Validation** (optional)

Visa Europe Technical Implementation Consultants assist in validating that the participants' systems can interact with Visa Europe in a VECSS environment for both incoming and outgoing files.

Note Validation may not be carried out in all test scenarios. The scope of the testing must be discussed and decided when defining the requirements of the project.

37.3.1.2 Components required

Members need the following components to perform testing using VMTS:

- Extended Access Server (EA Server)
- Edit Package

To facilitate testing, Visa Europe recommends that Members establish a method to run a test system comprising their hardware and software and a methodology to verify that the test transactions and reports are updating their systems as expected.

37.3.1.3 VMTS constraints

Capacity in VMTS is limited. Volume or stress testing is not available. Multiple services can be tested but are limited to a cumulative daily limit for each service. Processing Centres that support multiple Members are also limited to the same cumulative daily limit. Visa Europe Technical Implementation Consultants may request an exception to this limit on participants' behalf.

37.3.1.4 Acquirer tasks

For information on Acquirer testing tasks for new services or business enhancements, see the *VisaNet Business Enhancements Member Implementation Guide* for each service.

Acquirers may send samples of transaction types that apply to the new services or business enhancements. These include:

- Originals (TC 05, usage code 1)
- Credit vouchers (TC 06, usage code 1)
- Cash disbursements (TC 07, usage code 1)
- Reversals of drafts, credit vouchers and cash disbursements (TC 25, TC 26, TC 27, usage code 1)
- Representments (TC 05, TC 06, TC 07, TC 25, TC 26, TC 27, usage code 2)

Acquirers may also:

- Receive chargebacks (TC 15, TC 16, TC 17, usage code 1)
- Receive report records for selected services (TC 33)
- Request generic or customised TC 57 data capture service transactions, if applicable

The data represented in the transactions may be Custom Payment Service (CPS) or non-CPS, National Net Settlement (NNSS) and any other data type that is applicable to the Acquirer.

Note the following additional points:

- Merchants and Acquirers enrolled in the TC 33 service can test in VMTS.
- Acquirers convert TC 57s into TC 05s and submit these transactions to VECSS. Transactions destined for a responder BIN will receive chargebacks.

Acquirers can request generic or customised TC 57 data capture support. For more information, see the *VisaNet Certification Management Service Testing Guide for BASE II*.

Obtaining authorization test data

For Custom Payment Service (CPS) testing, Acquirers must use authorization test data in their VECSS test transactions to pass validation code edits. Unless an exception has been arranged with Visa Europe, Members are expected to submit clearing transactions based on and derived from authorization transactions. For VMTS, as for production, transactions submitted to VECSS for clearing must contain correctly formatted data.

Important For CPS, test data must be submitted within the specified timeframes.

To obtain authorization test data for VECSS, Acquirers can use one of the following methods:

- **VMTS for VEAS system testing**

Authorization data from VEAS system testing must be used for testing; it parallels production processing and provides production transaction identifiers and validation codes.

- **Visa Test System version 3 (VTS V.I.P.)**

VTS V.I.P provides simulation of VEAS processing for both dual message processing and the Single Message System (SMS). It is a testing system that simulates the processing of transactions between the Member hosts and VEAS.

- **Generating test authorization data**

Processors of Acquirers that use VECSS and that do not perform their own authorizations are encouraged to work with their authorization providers and Merchants to obtain authorization test data for more thorough testing. Output from authorization providers must be sent to Acquirers electronically along with actual deposit tapes from the Merchants.

- **Acquirer-generated authorization data**

Acquirers must perform VMTS for VEAS testing (with or without VTS V.I.P) to obtain Transaction Identifiers and validation codes that pass VMTS for VECSS testing edits.

Transaction Identifiers and validation codes used in production VECSS will not produce the same results if used in VMTS.

37.3.1.5 Issuer tasks

For information on Issuer testing tasks for new services and business enhancements, see the *VisaNet Business Enhancements Member Implementation Guide* for each service.

Issuers are sent sample transactions that apply to the new services or business enhancements.

These include:

- Originals (TC 05, usage code 1)
- Credit vouchers (TC 06, usage code 1)
- Cash disbursements (TC 07, usage code 1)
- Reversals of drafts, credit vouchers and cash disbursements (TC 25, TC 26, TC 27, usage code 1)
- Fee collection transactions and funds disbursement transactions (TC 10, TC 20 usage code 1)
- Multiple use transactions such as TC 33 and TC 50, usage code 1
- Representments (TC 05, TC 06, TC 07, TC 25, TC 26, TC 27, usage code 2)

The data represented in the transactions may be CPS or non-CPS, National Net Settlement (NNSS) and any other data type that is applicable to the requesting Issuer.

37.3.1.6 Success criteria

Participants must be able to send and receive transaction formats and new data elements for new services or business enhancements. For more information on the success criteria for new services or business enhancements, see the relevant testing sections in the *VisaNet Business Enhancements Member Implementation Guide* for each service.

To verify successful testing for a specific service, review the VisaNet Settlement Service (VSS) or Edit Package reports generated from testing. The reports must confirm the requirements in the testing sections in the *VisaNet Business Enhancements Member Implementation Guide* for each service.

If a transaction is returned, or in some cases, reclassified, testing may be regarded as unsuccessful and further work would be needed. Mismatching authorization and clearing data for mandatory fields would also produce an unsuccessful test result.

37.4 How the service works

VMTS provides the Batch Responder testing tool, which supports life-cycle testing. When Members submit transactions to valid responder BINs, the Batch Responder creates appropriate transactions that can include chargebacks and representments, and reversals.

Members can choose a customised file type to be created to segregate transaction test data from transactions originating from responder BINs.

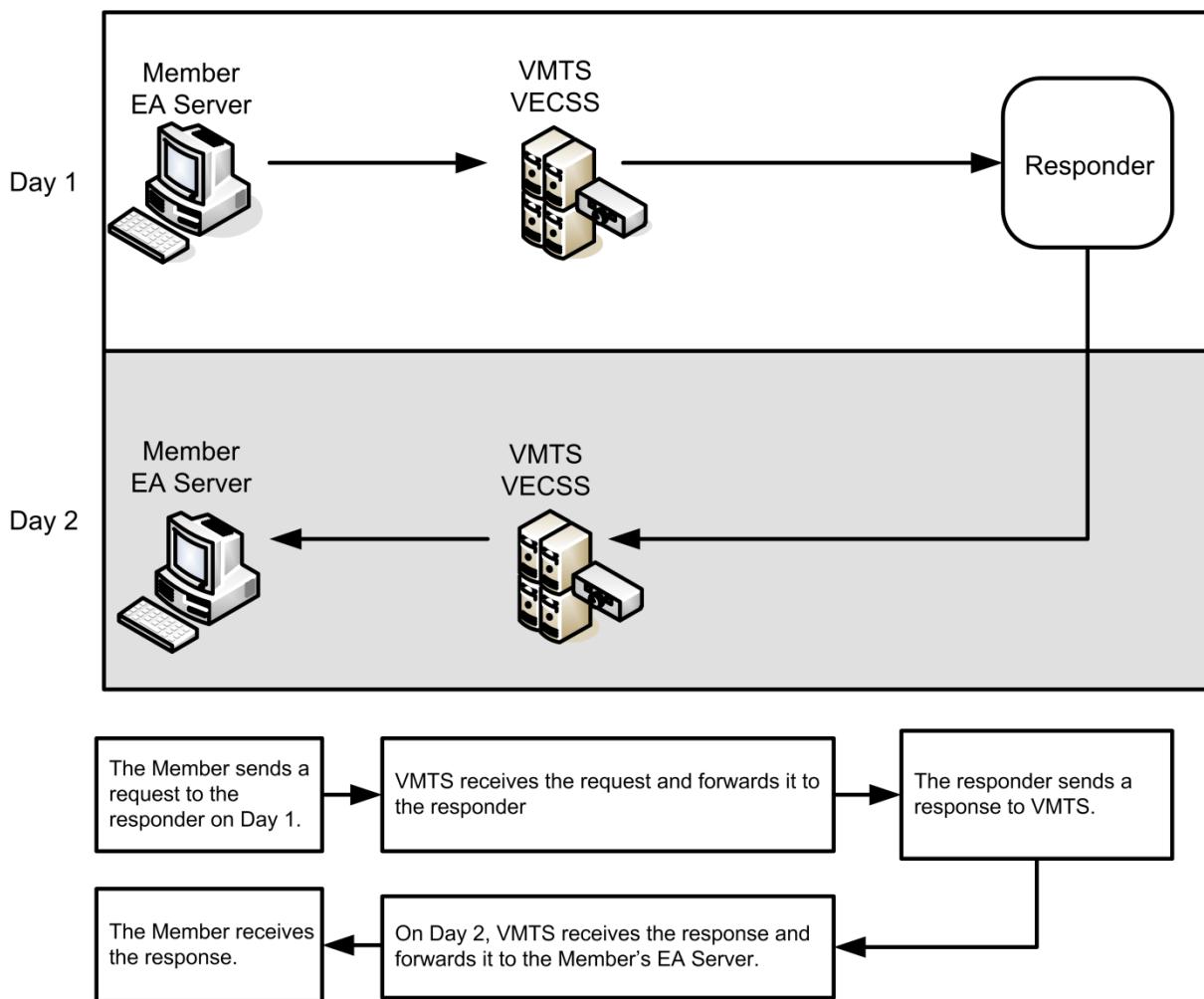
Members receive reports for submitted transactions in the same day's delivery cycle (or cycles). Because of the four-day cycle in processing transactions through Exception Manager (except for non-CPS), transactions are not validated and errors are not reported until the next cycle.

Transactions generated by the Batch Responder are not received until the fourth processing day cycle. Members must have transactions submitted to the Batch Responder to receive a response.

37.4.1 Batch Responder environment

The Batch Responder environment is illustrated in the following diagram.

Figure 81: The Batch Responder environment



The Batch Responder acts as an Issuer for Acquirer testing, and as an Acquirer for Issuer testing.

Example:

If an Acquirer submits an original sales draft (TC 05, usage code 1) to a valid Issuer responder BIN, the Acquirer receives a chargeback (TC 15, usage code 1) from the responder BIN.

By using the Batch Responder, Members can complete full transaction life-cycle testing (with the exception of conflict resolution), without coordinating their testing with other Members.

37.4.2 Responder BINs

Specific responder BINs, designated solely for Member testing, create original transactions and respond to exception transactions. The Batch Responder provides original transactions for Issuers and delivers them when requested throughout the scheduled test period.

For Members that want responses for life-cycle testing:

- Issuers must create exception items based on the originals received from the Acquirer responder BIN. Do not use reversals of chargebacks for this purpose.
- Acquirers must send originals to the responder BIN designated for the specific service; the Batch Responder will continue the life cycle.

These testing services are listed in the *VisaNet Business Enhancements Member Implementation Guide* for each service.

A BIN assigned to a specific country can be used as the destination BIN by another country for international testing.

Example:

An Acquirer in Singapore could send transactions to an Issuer responder BIN assigned to the UK. These BINs can be used for basic transaction testing, specific services, business enhancements and life-cycle testing. An original transaction, submitted using an account number for the responder BIN from the UK Issuer, will be returned to the Acquirer by the Batch Responder as a chargeback.

For a list of BINs used in Member testing, see the latest version of the *VisaNet Business Enhancements Member Implementation Guide*.

38 Visa Payment Controls

Visa Payment Controls (VPC) is a service for Issuers that allows their customers to establish rules on how their Visa cards may be used.

The service adds the rules to the authorization flow so that they are checked when transactions pass through the Visa Europe Authorization Service (VEAS).

Participating Issuers can offer the service to their customers and support them through a Visa Online (VOL) application. Issuers upgrade their own online banking system so that they and their customers can use VPC card management facilities directly, through the Visa Europe API.

The card rules are defined by Visa Europe, Issuers choose which rules they make available to their customers, and customers choose which of those rules to apply to their cards. A customer can control one or more cards from one Issuer.

38.1 Related information

The following documents contain further information about VPC:

- *Visa Payment Controls Member Implementation Guide*
- *Visa Payment Controls (VPC) API Technical Overview*
- *Visa Payment Controls Admin Console User Guide*
- *Visa Payment Controls Member Support Guide*
- *Visa Payment Controls Frequently Asked Questions - Issuer*
- *Visa File Transfer Initial Setup Guide*

38.2 Participation

Participation is optional for Issuers.

Issuers that choose to participate in VPC are required to undergo an onboarding process. Onboarding is the process of successfully integrating a new entity into the service, from both a service and technical perspective.

For detailed information about onboarding to VPC, see the *Visa Payment Controls Member Implementation Guide*.

38.3 How the service works

This section gives an overview of:

- The interfaces and user roles associated with VPC
- The card rules defined by Visa Europe
- How VEAS processing is impacted by VPC
- How the service is supported by the Issuer and Visa Europe

38.3.1 Interfaces and user roles

The following interfaces are used by VPC:

Table 48: VPC interfaces and users

	VPC interface	Used to	Used by
Issuer	Visa File Transfer (VFT)	Pre-register card Managers with VPC and make changes to their Card Manager accounts (when required)	Issuer VPC account change system The system or team in the Issuer's organisation that sets up and alters Card Manager accounts. For more information, see the <i>Visa File Transfer Initial Setup Guide</i> . Note If an Issuer is already using VFT for other Visa Europe services, they can use their existing VFT setup for VPC. VFT routes batch files to the appropriate service.
	Admin Console in VOL	View and update details on behalf of the Card Manager accounts in VPC	Issuer Customer Support team The team in the Issuer's organisation that supports the Card Managers. For more information, see the <i>Visa Payment Controls Admin Console User Guide</i> .
Customer	Card Management API	Administer card rules	Card Manager Someone who manages a portfolio of one or more Visa cards from an Issuer, setting rules as to how, when and where these cards can be used, as well as for what and for how much.

For more information on how these interfaces are implemented for VPC, see the *Visa Payment Controls Member Implementation Guide*.

38.3.2 Card rules

Visa Europe has defined the card rules for VPC. During onboarding, Issuers decide which of these rules they will offer their customers. Issuers can choose to offer all or a subset of the predefined rules to their customers.

Table 49: VPC Rules

Rule name	Description
Enable/disable card	<p>Enable or disable use of card. Disabling the card means that all transactions for it will be declined.</p> <p>Important Disabling cards is a useful feature for cards that are used infrequently (which the customer can enable when required) or are temporarily mislaid but not lost/stolen. This feature does not replace your lost/stolen card process. If the card is lost or stolen, the customer must report it to the Issuer according to the applicable guidelines.</p>
Balance Enquiry Allowed	Permit or prevent a Cardholder from initiating transactions that reveal the account balance.
Cash Allowed	Permit or prevent a Cardholder from withdrawing cash from the card (whether from an ATM or through the cash back service) or engaging in any sales transaction where the item or service obtained may be viewed as a form of cash.
Single Cash Transaction Limit	Prevent a Cardholder from withdrawing more than a specified value in cash in a single transaction.
Cumulative Weekly Cash Limit	Prevent a Cardholder from withdrawing more than a specified total value in cash in a single week.
Cumulative Weekly Total Limit	Prevent a Cardholder from exceeding a specified total value for all purchases and cash transactions (combined) in a single week.
Merchant Countries	<p>Prevent a card being used outside specific countries, which the customer can choose from a list.</p> <p>Note This rule has no effect upon mail order, telephone order and e-commerce transactions.</p>
Merchant Channel	<p>Limit the use of the card to one or more of the channels: face2face, internet, phone.</p> <p>If the channel used is not mentioned in the rule, the transaction will be declined. Certain transactions are exempt from this rule, see the <i>Visa Payment Controls Member Implementation Guide (MIG)</i>.</p>
Merchant Category Groups (MCG)	<p>Limit the use of the card to one or more of 25 VPC merchant category groups.</p> <p>If the merchant category code used is not part of an MCG mentioned in the rule, the transaction will be declined. For a list of VPC merchant category groups, see the <i>Visa Payment Controls Member Implementation Guide (MIG)</i>.</p>

A Card Manager accesses VPC functions through their Issuer's online banking system, which (via the use of the appropriate Visa Europe API calls) enables the Card Manager to perform the following actions:

- Manage cards (for example, change the Cardholder name)
- Display the rules allowed by their Issuer
- Create new rule sets (groups of rules tailored to the company's requirements)

- Edit existing rule sets
- Add a card to a rule set
- Manage account settings (for example, change a password or username)

38.3.3 VEAS processing

VEAS checks the primary account number (PAN) of every incoming authorization request. Where the transaction affects an account registered in VPC, the first phase of authorization will pass it through the VPC rules engine to see whether it qualifies under the rules configured by the customer's Card Manager.

The transaction undergoes all the usual preauthorization checks and continues through the normal authorization path. If the transaction is blocked by VPC or by another preauthorization check, VEAS will decline the transaction.

If there are no other, more severe reasons to deny approval, VEAS notifies the issuer via a 0120 or 0220 STIP advice message with field 63.4 - STIP/Switch Reason Code set to 9024.

In all cases, VEAS updates spend and transaction counters for the card, as well as record salient facts about the latest card usage.

38.3.4 Customer support

The Issuer's customer support team uses the VPC Admin Console in VOL to support the Card Manager. Once logged into the Admin Console, they can:

- Search for transactions performed on cards managed by a given Card Manager, and if the transaction was declined, identify which rules were triggered
- Search for Card Manager accounts and their cards and rule sets
- Make configuration changes on behalf of the Card Manager

Visa Europe Customer Support also has access to the VPC Admin Console, with the added capability of searching across all onboarded Issuers.

For more information, see the *Visa Payment Controls Admin Console User Guide*.

38.4 Process flows

This section gives a high-level overview of the process flows involved in VPC.

1. Onboarded Issuers promote the VPC service to their customers.

When a customer signs up for the service, the Issuer generates a request batch file that is transmitted to VPC using VFT. The batch file contains pre-registration data such as:

- Customer reference ID
The customer reference ID is the Issuer's unique identifier that ties the customer data together.
- Card details, such as name on card and PAN

2. If the batch file data is correct, VPC stores the pre-registration data.
Note It can take up to 24 hours for the data to propagate fully across the VPC service.
3. VPC returns a Response file to the Issuer to indicate whether the actions in the Request batch file were successful or not.
4. The customer's designated Card Manager accesses the Issuer's VPC card management functions through the Issuer's online banking system.
5. The Issuer's online banking system retrieves (through the use of Visa Europe supplied VPC APIs) and displays the relevant data for the Card Manager, including their cards and the available card rules.
6. The Card Manager configures their rule sets and adds their cards to them. The Issuer's online banking system sends the data to VPC through the appropriate VPC API calls.
7. VPC makes appropriate rule configuration changes to the VPC rules engine.
Note Card rule changes made through the APIs are typically applied to the rules engine within two minutes.
8. VEAS checks transaction authorization requests by performing several preauthorization checks. If it receives any requests for PANs registered in VPC, it also sends the request to the VPC rules engine.

If the rules engine blocks the transaction and this response is the highest priority of the pre-authorization checks, VEAS will decline the transaction. The resulting 0120/0220 Issuer advice will include a value of 9024 in field 63.4 - STIP/Switch Reason Code.

38.5 Key messages

The following VEAS messages are impacted by VPC:

- 0120/0220 - STIP advice messages

38.6 Key data fields

This section describes the key data field that is used by VPC. For detailed information about usage and values, see the Visa Europe technical specifications.

Data field 63.4 - STIP/switch reason code

This field contains a code that identifies why STIP responded for the Issuer or why the switch generated an advice message. If this field contains a value of 9024, it means a transaction was declined due to a VPC rule.

39 Visa Shortest Online Path Service

The Visa Shortest Online Path (VSOP) Service enables all Issuers that use Dual Message System Authorization (DMSA) and that issue both Visa and MasterCard card products to receive MasterCard authorization requests directly from the Visa Europe System, including purchase, cash and balance inquiry transactions. This service eliminates the need to route requests to Banknet (the MasterCard processing network) before they go to the Issuer.

If the Issuer is unavailable, stand-in processing (STIP) can be invoked according to Issuer-defined parameters, similar to the processing available to all cards.

Note For VSOP subscribers, the Visa Europe Authorization Service (VEAS) always sends MasterCard requests to issuers in Visa format. Since these BINs are connected to the Visa Europe System, Visa-to-MasterCard message format conversion is not necessary.

39.1 Related information

For additional information about the VSOP Service, see the following:

- *Introducing the Visa Europe System*
- *Introducing the Visa Europe Authorization Service*
- *Introducing Single Message System (SMS) and Dual Message System Authorization (DMSA) Transactions*
- *Introducing Single Message System (SMS) and Dual Message System Authorization (DMSA) Messages*
- *Introducing Stand-In Processing (STIP)*

39.2 Participation

The VSOP Service is available through the dual messaging system.

Participation is optional for Issuers.

To participate in the service, Members must meet the following requirements.

39.2.1 Testing and certification

Certification is mandatory for participation in the VSOP Service. The Visa Member Testing Service (VMTS) provides testing and certification assistance. To arrange for testing and certification, Members must contact Visa Europe Customer Support.

39.2.2 Planning and implementation

To participate in the service, Members must define their MasterCard account ranges in the Visa globals in the same way as their existing Visa BINs. In addition, to enable VEAS to translate and verify transactions containing PINs, Members must supply Visa Europe with

their encryption keys and establish links to existing encryption keys.

For more information, Members must contact Visa Europe Customer Support.

39.3 How the service works

The main steps in the VSOP Service are:

1. The Issuer establishes a BIN (or BINs) for its MasterCard transactions, and sets up its MasterCard account ranges to point to the BIN(s). The Issuer can also set up separate BINs for its PIN and no-PIN transactions and link to its existing encryption keys for PIN verification.
2. When VEAS receives a VSOP authorization request, if the Issuer is available, it routes the authorization request to the Issuer for a response. If the Issuer is not available, the request is routed to STIP for authorization.
3. In STIP, VEAS checks the Cardholder Database (CDB) Exception File for MasterCard entries. If a negative code is found, it declines the authorization request. If a negative code is not found, then regular Positive Cardholder Authorization Service (PCAS) checks are invoked.

Note When a Member lists a pickup record on the MasterCard Restricted Cardholder List (the equivalent to Visa's Card Recovery Bulletin (CRB)), the record is also included in the MasterCard Account Management System (AMS) file. The MasterCard AMS file is available to any MasterCard member for their 'under floor limit' use. Visa Europe also subscribes to this file and adds the records to the Visa CDB with a special action code.

4. To ensure that authorization and clearing meet MasterCard processing requirements, Visa passes proprietary MasterCard data in authorization responses. Subfield 62.17 is reserved for the Authorization Gateway transaction Identifier/MasterCard Financial Network Code (MasterCard DE63.1), which may be included in the 0110 authorization response at the Issuer's discretion.
5. The authorization response is sent to the Acquirer.

Note The VSOP Service supports only 0100 authorization requests and their 0110 authorization responses.

Acquirers that participate in the Visa Europe Multicurrency Service can, by default, send and receive their MasterCard transactions in the initially defined local currency. For information about this service, see [Multicurrency Service](#) on page 174.

VSOP participants can also separate the routing of PIN and no-PIN MasterCard transactions to different Processing Centres or Processing Endpoints using the PIN/No-PIN Split Routing Service option. For information about this service, see [PIN Routing Service](#) on page 211.

For basic information about STIP routing, see the *Introducing Stand-In Processing* document.

40 Visa Smart Debit/Credit Service

The Visa Smart Debit/Credit (VSDC) Service is a chip-based solution that enables participants to combine the functionality of debit, credit and prepaid products with the flexibility of chip technology. VSDC provides a globally interoperable payment service with a suite of optional risk control enhancements available only through chip technology. Chip cards help with:

- Reducing fraud by making it difficult to counterfeit or modify cards and transactions
- Increasing the security of offline transactions through checks that can validate the card and Cardholder offline
- Increasing the security of online transactions by providing a dynamic online cryptogram that is only valid for a single transaction
- Introducing new Cardholder verification methods
- Introducing new features and functionality to Visa products

To maintain global card payment interoperability EMVCo, an association of Visa, MasterCard, JCB and American Express (originally Europay, MasterCard and Visa) has developed a standard, EMV™ Integrated Circuit Card Specifications for Payment Systems. The EMV standard covers the terminal and the card side of chip card transactions - Integrated Circuit Cards (ICC) - at chip-reading devices.

The Visa Integrated Circuit Card Specification (VIS) and the Visa Contactless Payment Specification (VCPS) are separate Visa-specific application specifications based on the EMV standard that may be used to offer the VSDC Service.

For Acquirers using VSDC, dynamic data assists in complying with the Payment Card Industry Data Security Standard (PCI DSS), a worldwide security initiative to help organisations that process payment card data protect against credit card fraud, hacking and various other security vulnerabilities. Card authentication provides additional protection against counterfeit chargebacks.

For Issuers, VSDC provides access to multiple accounts and services on a single card. The service provides a range of debit, credit and prepaid chip card functions, allowing Issuers to customise these products to suit their markets and Cardholder needs.

40.1 Related information

For further information about the VSDC Service, see the following:

- *Acquirer Device Validation Toolkit (ADVT)*
- *EMV Common Payment Application Specification*
- *Payment Technology Standards Manual*
- *PIN Management for IC Cards Member Implementation Guide*
- *Transaction Acceptance Device Guide*
- *Transaction Acceptance Device Requirements*

- *Visa Smart Debit/Credit Certification Authority Technical Requirements*
- *Visa Smart Debit/Credit Implementation Guide for Acquirers*
- *Visa Smart Debit/Credit Implementation Guide for VIS Issuers*
- *Visa Smart Debit/Credit Personalization Specification*
- *Visa Smart Debit/Credit Personalization Assistant, Issuer User Guide*
- *VisaNet Certification Management Service (VCMS) Testing Guide - V.I.P., Member Version*
- *Visa Test System - V.I.P. User's Guide*
- *VisaNet Certification Management Service (VCMS) Testing Guide - BASE II, Member Version*
- *Dual Message System Authorization (DMSA) Technical Specifications*
- *Dual Message System Authorization (DMSA) Processing Specifications*
- *Single Message System (SMS) ATM Processing Specifications*
- *Single Message System (SMS) POS Processing Specifications*
- *Single Message System (SMS) POS Technical Specifications*
- *Single Message System (SMS) ATM Technical Specifications*
- *Dual Message System Clearing (DMSC) Technical Specifications*

40.2 VSDC features

VSDC features include:

- **Magnetic stripe data image** - comprises a near duplicate of the data on the physical magnetic stripe. This is a basic feature of any VSDC card. It represents the fundamental information needed for transaction processing and account access.
- **Online card authentication** - when a card and chip-reading device send a transaction online, the chip generates a cryptogram, the authorization request cryptogram (ARQC). The Issuer, or Visa on behalf of the Issuer, validates that the transaction came from a valid card and that key cryptogram data has not been changed. This is defined as online card authentication.
- **Issuer authentication** - to protect the Issuer's authorization response and to allow the card to validate that the response came from a valid Issuer, the Issuer, or Visa on behalf of the Issuer, may send a cryptogram, the authorization response cryptogram (ARPC), to be authenticated by the card.
- **Authorization controls** - an Issuer can set individual or group Cardholder limits that help determine the circumstances when transactions require online authorization. These controls help reduce exposure from higher risk accounts, especially in high floor limit environments. Limits are set during card personalisation and include:
 - Account usage control - determines whether a card can be used for International transactions, domestic transactions, or both types of transactions for each of the services provided by VSDC: goods and services, cash, cash back, and so on, and whether the card can be used at ATMs and/or point-of-sale/point-of-service (POS)

- Velocity check - offline counter limits - determines the number of transactions that can be processed offline before an online transaction is required
 - Velocity check - offline amount limits on transactions - determines the total amount for offline transactions that can be processed before an online transaction is required
 - Account effective and expiry date checking
 - New card check - if card is new, forces an online transaction
- **Cardholder Verification Method (CVM)** - a VSDC application is personalised with a list of the appropriate CVMs for a chip-reading device to use for a transaction. For example:
- Online PIN
 - Signature
- The VIS card specification also has two forms of Cardholder verification, which allow a PIN to be validated offline, at the POS:
- Offline plain text PIN
Chip-reading device sends the unencrypted PIN to the card where it is validated
 - Offline enciphered PIN
Chip-reading device encrypts the PIN using public key technology and sends it to the card where the card decrypts the PIN and then validates it
- It is also possible to vary the number of attempts a Cardholder may make on entering their PIN before the PIN is blocked:
- PIN try limit - set number of failed entries before an action is required
- **Issuer script updates** - provides the ability to change information on the debit or credit application without reissuing the card. A VIS card may support scripts for application block, application unblock, card block, PIN change/unblock functionality and commands for changing other data stored on the card. For example, Issuer script commands can:
- Change the Cardholder's PIN stored on the card for an offline PIN without reissuing the card
 - Control risk exposure by enabling you to block the card and can enhance customer service by providing a way to change the Cardholder's PIN at the POS
- **Offline data authentication** - the VIS card specification provides protection for data held on the card against alteration and manipulation and may help detect counterfeit cards. Several forms are available:
- Static Data Authentication (SDA) - verifies the integrity of the data elements stored in the card during personalisation. SDA is similar to Card Verification Value (CVV) processing in that it detects alteration of selected static data elements after personalisation. SDA provides protection without requiring an online message to the Issuer

- Dynamic Data Authentication (DDA) - provides the same functionality as SDA, and in addition, provides assurance to the chip-reading device that the card is genuine, and not a counterfeit copy
- Combined DDA/application cryptogram generation (CDA) - provides the same functionality as DDA, and in addition, validates that an intermediate device has not altered data between the card and the chip-reading device

Not all of these options are supported worldwide. Issuers in the Europe region are not allowed to issue cards containing or using SDA.

- **Full-chip data** - a VSDC full-chip data implementation currently includes up to 18 chip-specific data fields/tags in authorization, full financial, and clearing and settlement messages.

In the Europe region, Acquirers are mandated to support full-chip data and must be certified by Visa Europe.

Acquirers must ensure that their authorization services provide full-chip data support within data field 55 - VSDC Chip Data of their Visa messages.

40.2.1 Card types

Visa cards comprise the following EMV card types:

- The Visa Integrated Circuit Card Specifications (VIS) is the Visa-specific implementation of the EMV specifications.
- The Common Core Definition (CCD) is a newer EMV card type that contains the same data as the VIS card type but with expanded chip-to-Issuer processor communication, external data flow controls, and Issuer application and authentication data controls.

VIS and CCD capabilities include the following:

- An Acquirer must send VIS or CCD chip data in field 55
- An Issuer can send and receive VIS or CCD chip data in field 55 or in fields 130-149 using the expanded third bitmap format
- VIS and CCD chip data is eligible for both the card authentication and Issuer authentication features
- VIS and CCD transactions are eligible for the enhanced VSDC routing and stand-in processing (STIP) capabilities based on specific terminal or card verification results

An Issuer can issue both VIS and CCD compliant cards from the same BINs.

40.2.1.1 Format options for chip data

VSDC is supported in the Visa Europe Authorization Service (VEAS) by utilising specific data fields. An Acquirer must use field 55 to send and receive chip data. An Issuer can receive and send chip data in field 55, or by several fields contained in the third bitmap.

Regardless of the format used to submit chip data, VEAS converts the chip data into the format that is appropriate for the receiving Member, such as a conversion from field 55 to the third bitmap format.

40.2.2 VSDC supporting services

The following are additional optional services that are available to Members that use VSDC.

40.2.2.1 PIN Management Service

This service allows Cardholders to change or unblock PINs in VSDC cards. For more information, see [PIN Management Service](#).

40.2.2.2 integrated Card Verification Value (iCVV)

VSDC cards contain an image of the magnetic stripe data in the chip as well as a physical magnetic stripe. The magnetic stripe data in the chip and the physical magnetic stripe contain identical data, except that the 3-digit CVV on the chip's magnetic stripe image can be different from the CVV encoded on the physical magnetic stripe. When the chip's CVV is different from that on the physical magnetic stripe, it is referred to as an integrated Card Verification Value (iCVV).

The purpose of the iCVV is to protect against the copying of the magnetic stripe data from the chip for the creation of a counterfeit magnetic stripe card.

40.2.2.3 dynamic Card Verification Value (dCVV)

The dCVV is the Card Verification Value scheme for Visa contactless payment service transactions. Valid for DMSA and SMS, the service obtains Cardholder data from the card without physical card-and-terminal contact.

40.3 Participation

The VSDC Service is available through the dual and single messaging systems.

Participation is:

- Mandatory for Issuers and Acquirers of V PAY
- Optional for all other Members

Note All newly-installed devices that accept Visa cards and Visa Electron cards must be chip-reading devices.

To participate in the service, Members must meet the following requirements.

40.3.1 Requirements for Acquirers

To participate in the service, Acquirers must:

- Support VSDC devices - EMVCo type approvals level 1 and 2
- Capture and transmit full-chip data for all chip-initiated transactions from all chip-reading devices with active chip functionality
- Generate and send VSDC data in field 55 in authorization and full financial messages, and support the relevant chip data in clearing messages

40.3.2 Requirements for Issuers

To participate in the service, Issuers must:

- Receive VSDC data in the third bitmap or field 55 in authorization and full financial messages, and support the relevant chip data in clearing messages
- Place the magnetic stripe image (MSI), also known as Track 2-equivalent data, in the chip in all cards
- Perform card and Issuer authentication
- Ensure the VSDC application is configured to support Cardholder Verification Method (CVM), online card authentication, authorization controls
- Choose whether the VSDC application is configured to support offline authorization, Issuer authentication, and Issuer scripts

40.3.3 Testing and certification

Issuers and Acquirers must be certified to process VSDC transactions.

Acquirers need to be certified for their host processing, and must test their terminals before rollout and software update using the Acquirer Device Validation Toolkit (ADVT) set of test cards (contact chip-reading devices) and the Visa payWave Test Tool (VpTT) simulator (contactless devices).

Issuers must also establish parameters for stand-in processing (STIP) for Issuer available and unavailable conditions. Certification requirements include those for the third bitmap formats (Issuers only), field 55, and the contactless indicator.

40.3.4 Service monitoring

Service monitoring is not available for the VSDC Service.

40.3.5 Planning and implementation

For full planning and implementation support, contact Visa Europe Customer Support.

40.4 How the service works

All activity, except online processing, occurs offline and takes place between the card and the chip-reading device. Online processing occurs when the card and chip-reading device send the transaction online for Issuer authorization. Otherwise, the transaction proceeds offline, and is either approved or declined.

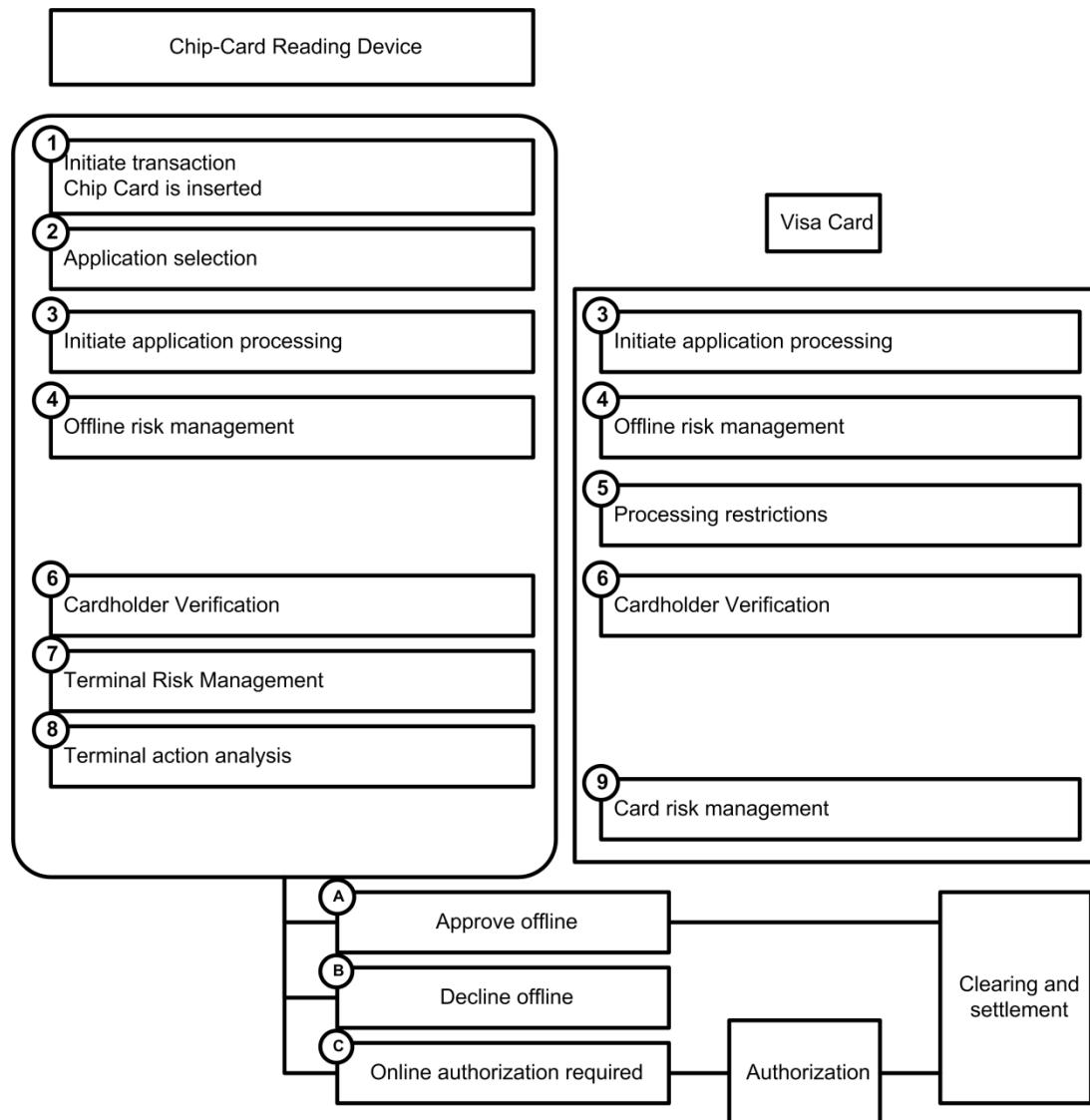
During processing of a VSDC contact transaction, the card remains in the chip-reading device. When the transaction is complete, the card is removed.

The steps involved in VSDC processing are illustrated in the following diagram and explained in the text that follows the diagram.

Note As the functions available depend on the card personalisation options selected by the Issuer, the chip-reading device may not perform all those listed.

The example relates to a chip card used at a chip-reading device.

Figure 82: How the VSDC Service works



- Initiate transaction** - the card is inserted in the chip-reading device.
- Application selection** - the chip-reading device identifies which applications are supported by the card and by the device. If there are no common applications, the terminal terminates the transaction.

If the card and the chip-reading device have only one application in common, the device uses that application. If there is more than one common application, then either:

- The Cardholder makes a selection from the list displayed on the chip-reading device, if Cardholder application selection is supported; or
- The chip-reading device selects the application with the highest priority; or
- The chip-reading device selects the application with the highest priority that does not require Cardholder confirmation

3. **Initiate application processing** - the chip-reading device signals to the card that a transaction is about to begin. The device sends any data requested by the card to the card.
 - The chip-reading device indicates whether the transaction is a domestic transaction or an International transaction. This affects the range of transaction data sent by the card to the chip-reading device
 - The card sends data to the chip-reading device indicating the type of functions and which offline risk management the card supports
4. **Offline risk management** - offline transaction checks are performed, if supported by the card and the chip-reading device. Offline data authentication is performed using one of the following methods:
 - Static Data Authentication (SDA), or
 - Dynamic Data Authentication (DDA), or
 - Combined DDA/application cryptogram generation (CDA)These checks ensure that the card has not been altered since it was issued. At the conclusion of offline data authorization, the chip-reading device records the results in the Terminal Verification Results (TVR) field.
If offline data authentication is not performed, the transaction must be processed online.
5. **Processing restrictions** - the chip-reading device performs the following checks:
 - Card effective/expiry date checking
 - Application usage control checking
 - Application version number checking
6. **Cardholder Verification Method (CVM)** - the chip-reading device interrogates the card to determine the most appropriate CVM to use for the transaction. The CVM employed is governed by the applicable payment scheme or processing rules and by the personalised Issuer-specified parameters of the card. The device or the Merchant verifies that the Cardholder is legitimate and the card is not lost or stolen. Verification methods include:
 - Online PIN
 - Offline plain text PIN - chip-reading device passes the PIN to the card unencrypted
 - Online enciphered PIN - chip-reading device encrypts the PIN before sending it to the card. The card then decrypts the PIN prior to performing validation
 - Cardholder signature

7. **Terminal Risk Management** – the chip-reading device performs checks based on the Acquirer risk control features in place. The results feed into the terminal action analysis, which determines whether the device will approve offline, decline offline, or send online. Checks include:
 - Merchant floor limit check
 - Random online transaction selection
8. **Terminal action analysis** - the chip-reading device assimilates the data, and based on the results, requests the card to generate one of the following cryptograms:
 - Approve offline - transaction certificate (TC)
 - Decline offline - application authentication cryptogram (AAC)
 - Online authorization required - authorization request cryptogram (ARQC)
9. **Card risk management** - enables the card to perform velocity checking and other risk management checks on behalf of the Issuer. The card may perform the following checks:
 - Previous transaction checks
 - New card checks
 - Velocity checks

After the card has completed the risk management checks, it determines what action to take based on the results of the checks, and on the type of cryptogram requested by the chip-reading device. It responds to the chip-reading device by supplying a cryptogram:

- Approve offline - TC
- Decline offline - AAC
- Online authorization required - ARQC

The chip-reading device acts on the card decision.

After the card generates the final cryptogram, the chip-reading device captures and stores the transaction information. This information is submitted during the regular clearing and settlement process.

40.4.1 A - Approve offline

The Acquirer submits the approved transaction to the Visa Europe System for clearing and settlement.

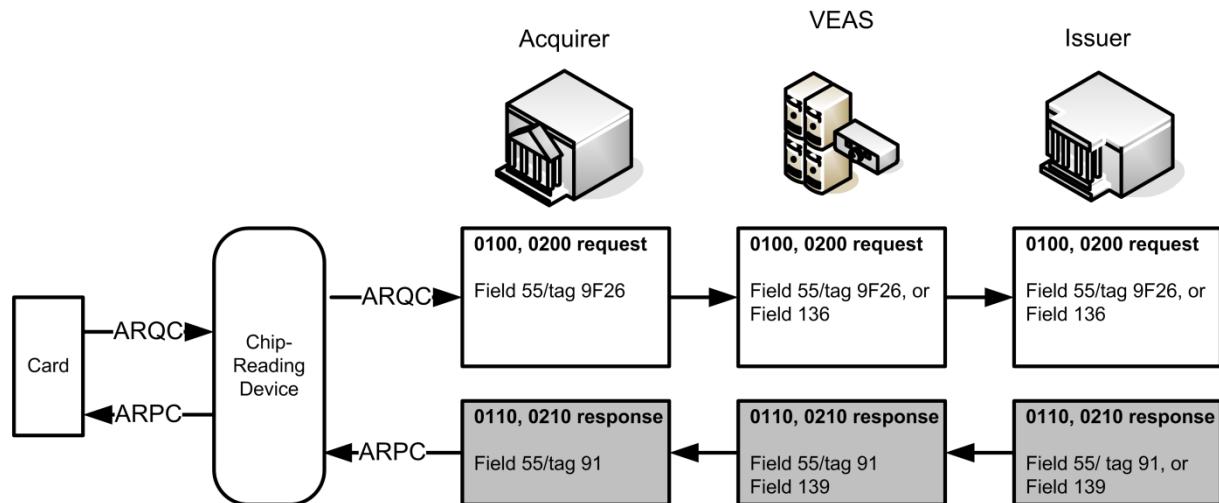
40.4.2 B - Decline offline

The details of offline declines are only sent to the Issuer if the Issuer and Acquirer support offline advice messages.

40.4.3 C - Online authorization required

Online card and Issuer authentication comprise the following steps.

Figure 83: Online authorization for the VSDC Service



1. The card generates the Authorization Request Cryptogram (ARQC). A cryptogram is the result of card, terminal and transaction data encrypted by a secret key. The cryptogram is unique for each transaction. The chip card sends the cryptogram and the data to the chip-reading device.
2. The chip-reading device forwards the cryptogram, along with the data elements used by the chip to create the cryptogram, and other card-defining data such as the card verification result, to the Acquirer.
3. The Acquirer formats this data into a 0100 authorization request or a 0200 financial message and sends the message to VEAS.
4. VEAS receives the message and routes it to the appropriate Issuer.

Under certain defined conditions, and if the Issuer is unavailable, VEAS may act on behalf of the Issuer. For each defined condition (there are currently 29 for VIS cards, and 33 for CCD cards) the Issuer specifies whether to force the authorization request to the Issuer, or have STIP respond with an approval response or a decline response.

5. The Issuer performs the card authentication process. The Issuer sends the data to its host security module (HSM), which executes the algorithm to validate the ARQC.

The HSM uses the card's derivation key index to locate the master derivation key, which is used to derive the unique derivation key used by the card to generate the cryptogram. The HSM takes the master derivation key along with the primary account number and the card sequence number and derives the unique derivation key.

The Issuer uses the unique derivation key to generate a comparison cryptogram. The cryptogram generated by the HSM is compared to the cryptogram in the authorization request and a pass or a fail response is returned. A pass means that the card authentication is successful.

6. The Issuer sends the response to VEAS. If the Issuer uses the Issuer authentication feature, the Issuer generates the Authorization Response Cryptogram (ARPC) and includes the cryptogram in the response to the Acquirer.
The ARPC is generated using the ARQC, the response code, and the unique derivation key. The Acquirer receives the authorization response and sends it to the chip-reading device. The device forwards the authorization response with the ARPC to the card.
If VEAS performs this service, the Issuer returns the response with only the card authentication result. VEAS generates the ARPC and includes it in the response to the Acquirer.
7. The card validates the Issuer by generating an ARPC and comparing it to the one provided by the Issuer in the response. A match means the authentication is successful and the card knows it is communicating with the correct Issuer. Issuers can have VEAS perform Issuer authentication for every transaction, for only those transactions processed by STIP, or for no transactions.

40.4.4 DMSA routing and STIP

Certain VSDC-specific data field conditions in the request influence the VEAS decision to route VSDC transactions to the Issuer or to STIP. If card authentication is successful but the Issuer is unavailable, VEAS forwards the transaction to STIP for an approval or decline decision based on Issuer-specified parameters.

40.4.5 SMS routing and STIP

VEAS routes all SMS VSDC transactions to available Issuers. VEAS forwards a transaction to STIP only if the Issuer is unavailable. STIP processes the transaction according to Issuer-defined parameters.

40.4.6 Fallback transaction

Fallback transactions are transactions read from the magnetic stripe (field 22 - Point-of-Service Entry Mode Code = 90) of a chip card when used at a chip-reading device.

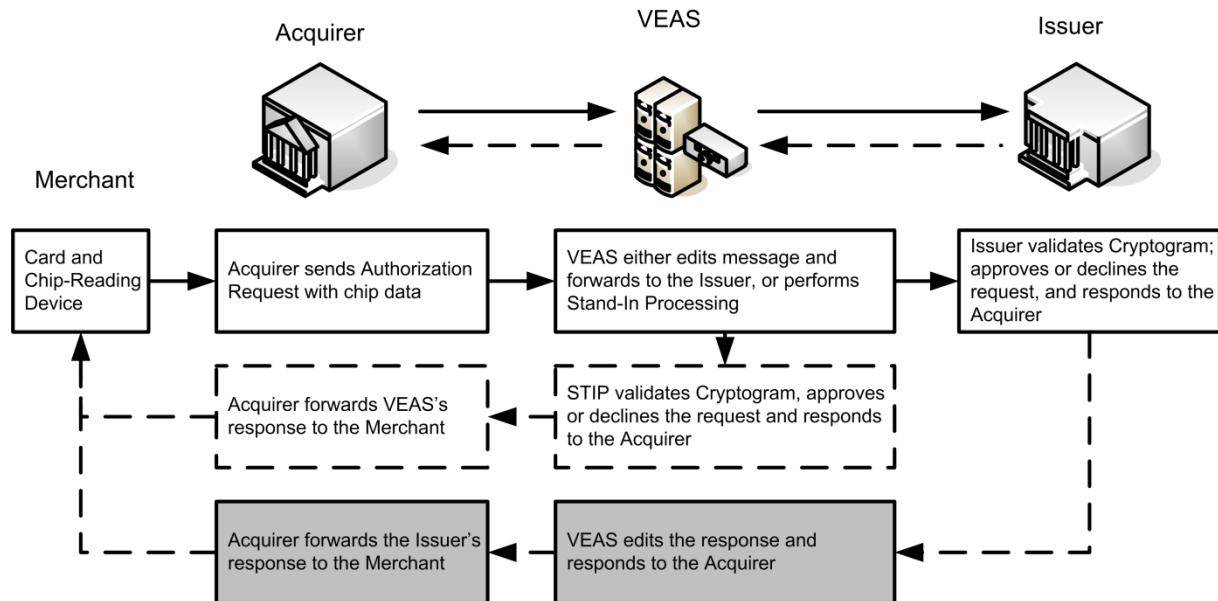
If the chip-reading device cannot read the chip, the Merchant is allowed to swipe the card for a magnetic stripe-based transaction.

There may be situations where both the chip data and the magnetic stripe data of the card cannot be obtained by the terminal. In this case, a key-entered fallback transaction may be initiated.

40.5 Process flow

The following steps comprise the processing flow when both an Acquirer and Issuer fully participate in the VSDC Service.

Figure 84: Process flow for the VSDC Service



1. The card and chip-reading device perform VSDC processing and for online transactions, the VSDC data is sent to the Acquirer.
2. The Acquirer formats the authorization request using the chip data, including the ARQC.
3. VEAS validates the message content and structure, then does one of the following:
 - Edits (converts message format from field 55 to the third bitmap), validates the ARQC and provides the result (if requested by the Issuer) and forwards to the Issuer; or,
 - Drops the chip data and forwards to the Issuer; or,
 - Performs stand-in processing and responds to the Acquirer on the Issuer's behalf
4. The Issuer validates the cryptogram or reviews the result from VEAS. It approves or declines the transaction and returns the results in the authorization response. The response may include the ARPC.
5. VEAS forwards the response from the Issuer to the Acquirer. If there is no ARPC in the response, VEAS may generate the ARPC and send it in the response to the Acquirer.
6. The Acquirer forwards the response received via VEAS to the Merchant.
7. The chip-reading device sends the transaction response to the card.

40.6 Key messages

The following table lists the DMSA and SMS message types valid for VSDC processing:

- 0100/0110 POS authorization
- 0100/0110 POS account verification

- 0100/0110 ATM cash disbursement
- 0100/0110 ATM balance inquiry
- 0120 /0130 STIP or information advice
- 0200/0210 full financial transaction
- 0200/0210 ATM balance inquiry
- 0220/0230 adjustment
- 0220/0230 representment
- 0400/0410 reversal
- 0422/0432 chargeback
- 0422/0432 chargeback reversal
- 0620/0630 information message

40.7 Key data fields

The following key data fields are used to identify a VSDC Service authorization or full financial request. For detailed information, see the Visa Europe technical specifications.

Data field 22 - Point-of-Service Entry Mode Code

This data field contains a code indicating the method used to enter the account number and card expiry date, and for a chip-reading device, the device's PIN capture capability.

Data field 23 - Card Sequence Number

This data field contains the number assigned to a specific card, personalised on the chip card by the Issuer, when two or more cards are associated with a single account number.

Data field 35 - Track 2 Data

This data field contains the information coded on track 2 of the magnetic stripe, or the image of the stripe as encoded in the chip.

Data field 39 - Response Code

This data field contains a code that defines the response to a request or message disposition. It is present in 0110 and 0210 responses and in 0120 and 0220 advices, in 0220 Acquirer deferred clearing advices, and in 0620 chip-based informational advices.

Data field 44.5 - CVV/iCVV Results Code

This field contains a Visa-defined code that indicates CVV or iCVV results.

Data field 44.8 - Card Authentication Results Code

This data field contains a Visa-defined code indicating card authentication results. If VEAS performs card authentication on behalf of an Issuer, an Issuer can decide to receive the results in this field in authorization and full financial requests.

Data field 45 - Track 1 Data

For a contact VSDC transaction, this field contains the track data from the chip image.

Data field 55, Usage 1 - VSDC Chip Data

This data field is used for transmitting chip data in a tag-length-value (TLV) format. Acquirers are mandated to use this format, but Issuers may choose to receive the data in the third bitmap.

Data field 60.2 - Terminal Entry Capability

For VSDC transactions, this field contains the following code:

5 - Chip-capable terminal

Data field 60.3 - Chip Condition Code

This data field contains a code that provides information about fallback transactions which are initiated from the magnetic stripe of VSDC cards at VSDC devices.

Data field 60.6 - Chip Transaction Indicator

This data field contains a code indicating a VSDC transaction.

Data field 60.7 - Card Authentication Reliability Indicator

This data field contains a code indicating that an Acquirer or Issuer is inactive for card authentication.

41 Visa Token Service

The Visa Token Service is a payment token service that complies with the standards defined by the *EMV Payment Tokenisation Specification - Technical Framework*. A payment token is a surrogate for a primary account number (PAN). The token replaces the PAN in transaction processing, thereby reducing the risk of a Cardholder's sensitive payment information being compromised.

Payment tokens issued by the Visa Token Service support the following transaction types:

- **Visa payWave for Mobile payments**
A payment token provisioned to a mobile device can be used to make contactless payments at any acceptance device that supports Visa payWave.
- **Application-based e-commerce payments**
A transaction where a mobile application is able to use a payment token provisioned to a mobile device to perform a payment, without the need to request the user to enter payment card data or use card data stored on file.
- **E-commerce payments**
Tokens are not restricted to usage with particular consumer devices and can be used for standard e-commerce transactions. For example, a digital wallet provider can use payment tokens for browser-based payments via any device where a Cardholder can access their wallet.

The *EMV Payment Tokenisation Specification - Technical Framework* defines a number of roles that are relevant to the payment token service offered by Visa Europe:

- **Token Service Provider**
An entity that provides a payment token service by providing payment tokens to registered Token Requestors, linking the payment token to the payment card details provided in the request for a token. The Token Service Provider generates, issues and maintains tokens. It is also responsible for detokenising the token during transaction processing.
The Visa Token Service fulfils the role of a Token Service Provider.
- **Token Requestor**
A Token Requestor is an entity that has registered with a Token Service Provider to request payment tokens. Entities that may wish to register as a Token Requestor include Issuers, card-on-file Merchants, digital wallet providers, Acquirers and payment service providers operating on behalf of Merchants.

For more information see the *Visa Token Service Product Overview*.

41.1 Related information

The following documents contain further information about the Visa Token Service:

- *Visa Token Service Product Overview*
- *Visa Token Service Introduction for Acquirers*
- *Visa Token Service Introduction for Issuers*
- *Dual Message System Authorization (DMSA) Technical Specifications*
- *Dual Message System Clearing (DMSC) Technical Specifications*

The following document contains further information about Visa contactless payments:

- *Visa Contactless Payment Specification*

The following document contains further information on EMVCo standards for payment token services and is available from EMVCo:

- *EMV Payment Tokenisation Specification: Technical Framework*

41.2 Participation

Participation in the Visa Token Service is:

- Mandatory for Acquirers
- Optional for Issuers

41.2.1 Acquirer participation

Acquirers must be capable of processing transactions conducted using payment tokens.

There are two options for Acquirer participation:

- Passive participation
 - All Acquirers are by default passive participants. They process token-based payment transactions as they would any other valid Visa payment.
- Active participation
 - Acquirers can choose to be an active participant in the service. They will send and receive additional token-related information in the authorization messages for each payment token transaction that they process.

For more information, see the *Visa Token Service Introduction for Acquirers*.

41.2.2 Issuer participation

Issuers that choose to participate in the Visa Payment Token Service can enable their Cardholders to use tokenised instances of their cards in certain payment environments. To participate, Issuers must complete service participation agreements.

For more information, see the *Visa Token Service Introduction for Issuers*.

41.2.3 Testing and certification

Testing and certification are required for active Acquirers and all Issuers that choose to participate in the service.

41.3 How the service works

The Visa Token Service fulfils four functions:

- Service enrolment
- Payment token provisioning
- Transaction processing
- Payment token lifecycle management

41.3.1 Service enrolment

Before Visa Europe can commence issuing payment tokens, Members that have completed service participation agreements must:

- Provide Visa Europe with the card account ranges that they wish to make eligible for payment tokenisation and identify, with the assistance of Visa Europe, the token BIN ranges that will be assigned to tokenised instances of their cards
- Select token provisioning rules
 - Issuers can configure a rule set that defines how requests for payment tokens are dealt with during provisioning. For example, they can configure rules that define when a request for a token should be automatically declined, or when additional Cardholder authentication is required.
- Select token lifecycle management options
 - For more information, see *Payment token lifecycle management* on page 329.
- Provide card metadata and terms & conditions
 - Issuers must provide Visa Europe with card metadata, such as logos and card background colour, as well as customised terms & conditions text.
- Provide cryptographic key management information
 - Issuers must provide Visa Europe with up-to-date cryptographic keys for all eligible account ranges.
- Configure Visa Token Service web services
 - Issuers can opt to use Visa Token Service web services during token provisioning and token lifecycle management. During service enrolment, these services must be identified, configured and cryptographic keys and key certificates exchanged.

Once the above information has been submitted, and the Member has completed testing and certification requirements, Visa Europe proceeds to enable the Member to interact with the payment token service platform. For more detailed information, see the *Visa Token Service Introduction for Issuers*.

41.3.2 Payment token provisioning

When the Visa Token Service receives a payment token request from a valid Token Requestor, the process of payment token provisioning begins. This section gives a high-level description of how the service provisions payment tokens to a mobile device.

Note For more information about how tokens are provisioned for other use cases (for example, digital wallets), see the *Visa Token Service Product Overview*.

1. The payment token service receives a token request from a Token Requestor.
2. Visa Europe checks that the card details belong to a valid account range that is eligible for use with the service.
3. Visa Europe assesses the valid card against rules that the Issuer has configured that indicate whether or not a token request should be:
 - Approved
 - Declined
 - Subject to additional Cardholder identification and verification
4. Once the rules have been run, Visa Europe sends a 0100 token activation request message to the Issuer via the Visa Europe Authorization Service (VEAS), containing information from the Token Requestor (such as the Token Requestor's account score for the Cardholder) and information derived from the Issuer's rules.
5. The Issuer sends a 0110 token activation request response message indicating one of the following:
 - Unconditional approval - provision token and activate immediately
 - Conditional approval - provision token but do not activate until additional Cardholder verification has been performed
 - Decline - do not provision token
6. Visa Europe applies any service level business rules (which might, for example, change an Issuer's unconditional approval to a conditional approval) and returns a final response to the Token Requestor.

If the final decision is either an unconditional approval or a conditional approval, Visa Europe sends provisioning data scripts to the Token Requestor for delivery to the payment application in the mobile device.

- If an unconditional approval is granted, the payment token is activated in the vault, and the Token Requestor is informed.
- If a conditional approval is granted, the Token Requestor prompts the Cardholder to initiate step-up authentication (for example, requesting a one-time password). Once the authentication step has passed, the payment token can be activated and the Token Requestor informed.

41.3.3 Transaction processing

A transaction initiated with a payment token is processed in the same manner as a transaction initiated with a PAN. However, Acquirers that choose to actively participate in the service must be prepared to receive additional token-related data in authorization and clearing messages.

41.3.3.1 Issuers

Issuers that participate in the payment token service must be prepared to receive payment transactions containing token data. Issuers receive all the information they need to identify that a token was used to initiate a payment transaction, what the token value is, the channel (for example, Visa payWave for mobile or application-based e-commerce) it was used in and information about any Cardholder verification performed during the payment. For more detailed information, see the *Visa Token Service Introduction for Issuers*.

41.3.3.2 Acquirers

Acquirers that do not actively participate in the payment token service do not need to change their business processes. Visa Europe identifies the PAN from the token and performs authorization and clearing processes as normal. However, these Acquirers should be aware that there are some fields and values in authorization and clearing messages that relate specifically to the payment token rather than the PAN.

Acquirers actively participating in the service must ensure that they are able to process fields and values containing token data. They will receive information about the token in the authorization response and must also be capable of submitting POS clearing messages with additional token-specific data.

For more information on the fields impacted, see the *Visa Token Service Introduction for Acquirers*.

41.3.4 Payment token lifecycle management

The Visa Token Service provides participating Issuers with a number of ways to manage payment tokens linked to their cards:

- The payment token service API
A web service integration between Issuers and the payment token service that allows each party to call payment token web services operated by the other and to receive responses.
- 0302 token maintenance file messages via VEAS
Visa Europe system messaging using message formats that are specific to the payment token service. Issuers can send requests to and receive responses from the payment token service.
Note Not available to Issuers that choose the Easy Token transaction processing option.

- **Visa Online Service (VOL)**

Issuers can use VOL to access Visa Europe payment token lifecycle management functionality.

These options provide the following functions:

- **Token file maintenance**

Issuers can request that the service changes the status of a token on their behalf, for example, deactivate, suspend or resume a token.

- **PAN file maintenance**

Issuers can change details of one of their cards that are held within the system, for example, due to a replacement card being issued.

- **Token inquiry**

If an Issuer requires additional information about a payment token or a card, they can submit a message with request data that contains the payment token value or the PAN or the PAN reference ID:

- If the request data contains a payment token number, they will receive detailed data related to the payment token
- If the request data contains a PAN or PAN reference ID, they will receive the token number of every payment token linked with that card.

- **Card metadata update**

Once a token has been issued, if the underlying card product changes, Issuers can change some details (for example, the card art) relating to the token. The Token Requestor forwards the updates to the mobile device where the token is stored.

For more information on payment token management, see the *Visa Token Service Introduction for Issuers*.

41.4 Process flows

This section gives a high-level overview of the process flows involved in the Visa Token Service for device-based tokens. For information about other use cases (for example, digital wallets), see the *Visa Token Service Product Overview*.

41.4.1 Obtaining a payment token

1. Cardholder purchases a device that is compatible with Visa Europe's standards for mobile devices.
The mobile device must contain a payment application approved by Visa Europe to which the payment token service can provision a token.
2. Cardholder provides Token Requestor with their card details.
If the Token Requestor already has the card details on file, they may ask the Cardholder to confirm which card they wish to load onto their phone. Alternatively, the Cardholder can provide card details by, for example, using their mobile device to take a photo of

their card, typing in their card details, or touching their NFC-capable card on their NFC phone.

3. Token Requestor sends a token request to Visa Europe.

4. Visa Europe initiates token provisioning processing.

For more information, see [Payment token provisioning](#) on page 328.

5. The Token Requestor provisions the payment token onto the Cardholder's mobile device.

If the token that is provisioned to the device is not activated, additional Cardholder identification and verification may be required.

41.4.2 Making a payment using Visa payWave for mobile devices

A Cardholder that has obtained a payment token can choose to use a mobile device to pay for a purchase at a Visa payWave acceptance device.

1. Cardholder presents their mobile device to a Visa payWave acceptance device.

2. The Visa payWave Merchant forwards the transaction containing the payment token to the Acquirer.

3. The Acquirer sends the transaction containing the payment token to Visa Europe.

4. Visa Europe detokenises the payment token to identify the PAN and forwards the transaction containing the PAN (and optionally the full token data) to the Issuer for authorization.

5. The Issuer authorizes the transaction based on the PAN and returns the transaction to the Acquirer via Visa Europe.

Visa Europe replaces the PAN with the token and, depending on their level of participation in the service, returns additional token data to the Acquirer.

6. The Acquirer informs the Visa payWave Merchant of the outcome.

7. The Visa payWave Merchant informs the Cardholder of the outcome.

41.4.3 Making an application-based e-commerce purchase

A Cardholder that has obtained a payment token can choose to use a tokenised card to make a payment for an application-based e-commerce purchase through a Merchant application integrated with a Visa-approved mobile payment application.

1. Cardholder purchases item or service through a Merchant application on their device using their tokenised card.

2. The e-commerce Merchant forwards the transaction containing the payment token to the Acquirer.

3. The Acquirer sends the transaction containing the payment token to Visa Europe.

4. Visa Europe detokenises the payment token to identify the PAN and forwards the transaction containing the PAN (and optionally the full token data) to the Issuer for authorization.

5. The Issuer authorizes the transaction based on the PAN and returns the transaction to the Acquirer via Visa Europe.

Visa Europe replaces the PAN with the token and, depending on their level of participation in the service, returns additional token data to the Acquirer.

6. The Acquirer informs the e-commerce Merchant of the outcome.
7. The e-commerce Merchant informs the Cardholder of the outcome.

41.5 Key Visa Europe System messages

For detailed information about the authorization and clearing messages used by the Visa Token Service, see the following documents:

- *Dual Message System Authorization (DMSA) Technical Specifications*
- *Dual Message System Clearing (DMSC) Technical Specifications*

41.5.1 Authorization

The following VEAS messages are key to the Visa Token Service:

- 0100/0110 - Token activation request and response messages
- 0120/0130 - Token STIP advice and response messages
- 0302/0312 - Token maintenance file request and response messages
- 0620/0630 - Issuer token notification advice and response messages

41.5.2 Clearing

The following are the key clearing record changes for the Visa Token Service:

- TC x5, x6, Draft Data, TCR 0, positions 5-20
Contains the payment token value, not the PAN.
- TC x5, x6, Draft Data, TCR 0, position 160
Contains the Cardholder ID Method.
- TC x5, x6, Draft Data, TCR 1 Additional Data, positions 5-16
Contains the token assurance level, if available.
- TC 52 Request for Copy, TCR 1, positions 88-103
Contains the token.
- TC 40 Fraud Advice, TCR 2, positions 146-161
Contains the token (first 16 digits).
- TC 40 Fraud Advice, TCR 2, positions 162-164
Contains the remainder of the token, if longer than 16 digits.
- TC x5, x6, Draft Data, TCR 5 Payment Service Data, positions 150-165
Contains the token used to perform the transaction.

- TC x5, TC x6, Draft Data, TCR 7 Chip Card Transaction Data
Contains data generated by the token during transactions conducted using Visa payWave for mobile.

41.6 Key data fields

This section lists the key data fields that are used by the Visa Token Service. For detailed information about usage and values, see the Visa Europe technical specifications.

Data field 2 - Primary Account Number

This field contains the payment token value, not the PAN, in the incoming authorization request from the Acquirer. In the authorization request that the service forwards to the Issuer, the payment token value is replaced with the PAN.

Data field 4 - Amount Transaction

This field is used in token activation requests.

Data field 7 - Transmission Date and Time

This field contains the date and time when the token activation request was created.

Data field 11 - System Trace Audit Number

This field contains a number assigned by the message initiator that uniquely identifies a transaction.

Data field 14 - Date, Expiration

This field contains the expiry date of the payment token.

Data field 22 - Point-of-Service Entry Mode Code

This field does not contain values specific to the payment token service, however, a payment token can only be used with certain Point-of-Service Entry Mode Codes.

Data field 23 - Card Sequence Number

This field is required for chip-read transactions; it contains the sequence number of the token, not the linked card.

Data field 35 - Track 2 Data

This field contains data based on the token, not the underlying card.

Data field 37 - Retrieval Reference Number

This field contains a value that is used with other key data elements to identify and track all messages related to a transaction.

Data field 39 - Response Code

This field is used in token activation requests to indicate whether or not the request has been approved (conditionally or unconditionally) or declined.

Data field 44 – Additional Response Data

This field contains miscellaneous data needed in a response message.

Data field 44.5 - CVV/iCVV Results Code

This field contains a code indicating the results of validating the iCVV provided by the token.

Data field 44.8 - Card Authentication Results Code

This field contains the results of qVSDC processing with the token.

Data field 44.13 - CAVV Results Code

For application-based e-commerce transactions, Visa Europe will verify token data in field 126.9 and provide the results to the Issuer in field 44.13.

Data field 44.15 - Primary Account Number, Last Four Digits for Receipt

This field contains the last four digits of the PAN linked with the token.

Data field 45 - Track 1 Data

This field contains data based on the token, not the underlying card. If both Track 1 and Track 2 (field 35) are present in a message, VEAS gives preference to Track 2.

Data field 55 - Usage 1 and Usage 2

Acquirers must submit this field when token data is present.

Data field 60 - Additional POS Information

- Field 60.6 - Chip Transaction Indicator
 - Contains a value, set by VEAS and not the Acquirer, when chip-based Visa token processing has occurred.
- Field 60.8 - Electronic Commerce Indicator
 - Contains the value provided by Acquirer, as configured during token provisioning.

- Field 60.9 - Cardholder ID Method Indicator

Indicates the type of Cardholder authentication performed for the transaction.

Data field 62.23 - Product ID

This field contains the product ID of the card linked to the token in the authorization response.

Data field 63.3 - Message Reason Code

This field contains a value indicating that the message relates to the creation of a token and all token status changes.

Data field 63.4 - STIP/Switch Reason Code

This field contains a code that indicates that STIP processed the transaction because it was declined by the token provisioning service.

Data field 70 - Network Management Information Code

This field contains a code that defines the type of network management required.

Data field 91 - File Update Code

This field contains a value that specifies the type of file processing required. It is used in 0302/0312 messages relating to token and PAN maintenance files.

Data field 101 - File Name

This data field is used in all 03xx messages.

Data field 123, Usage 2 - Verification & Token Data (TLV format)

This field can contain the following datasets:

- Dataset ID 66, Address verification data
- Dataset ID 67, Verification data results
- Dataset ID 68, Token data

Data field 125, Usage 2 - Supporting Information (TLV format)

This field contains information relating to the mobile device used to make the transaction. It is used in token activation messages, token maintenance file requests and token notification advices.

Data field 126.9 - Usage 3: 3-D Secure CAVV, Revised Format

This field contains security data generated by the token and is used in application-based e-commerce transactions.

Data field 127 - Terms & Conditions, Usage 2

This field contains data identifying the set of terms and conditions that were accepted by the Cardholder during token provisioning.

Data field 127.PAN - PAN File Maintenance (TLV format)

This field contains the replacement PAN when the existing PAN in data field 2 - Primary Account Number is replaced by a new PAN. The field also contains the expiry date of the new PAN.