RPKI Engine

1.0

Generated by Doxygen 1.6.3

Mon Apr 19 19:43:58 2010

Contents

1 RPKI Engine Reference Manual **1**

2 Overview **2**

2.1 Terminology 2

2.2 Programs 3

2.3 rpkid 4

2.4 pubd 4

2.5 rootd 5

2.6 irdbd 5

2.7 smoketest 5

2.8 yamltest 6

3 Further Reading **6**

4 Installation Guide **6**

5 Configuration Guide **9**

5.1 myrpki.conf 9

5.2 Other configuration files and options 14

5.3 Common Configuration Options 14

5.4 rpkid.conf 15

5.5 irdbd.conf 16

5.6 pubd.conf 17

5.7 rootd.conf 19

5.8 smoketest.conf 20

5.9 smoketest.yaml 20

6 Left-Right Protocol **22**

6.1 initiated by the IRBE 22

6.1.1 <self/> object 23

6.1.2 <bsc/> object 25

6.1.3 <parent/> object 26

6.1.4 <child/> object 28
6.1.5 <repository/> object 28
6.1.6 <route_origin/> object 29
6.2 Operations initiated by the RPKI engine 31
6.2.1 <list_resources/> messages 31
6.3 Error handling 32

7 Publication protocol **33**
7.1 Publication control subprotocol 33
7.1.1 <config/> object 33
7.1.2 <client/> object 34
7.2 Publication subprotocol 34
7.2.1 <certificate/> object 35
7.2.2 <crl/> object 35
7.2.3 <manifest/> object 35
7.2.4 <roa/> object 35
7.3 Error handling 35
7.4 Additional access control considerations. 36

8 SQL database schemas **37**
8.1 rpkid SQL schema 39
8.2 pubd SQL Schema 44
8.3 irdbd SQL Schema 45

9 BPKI model **47**

10 The myrpki tool **50**
10.1 Getting Started -- Overview 51
10.2 Getting started -- Hosted case 53
10.3 Getting started -- Self-hosted case 54
10.4 started -- Hosting case 55
10.5 Getting Started -- "Pure" hosting case 55
10.6 Troubleshooting 56

10.7 Known Issues 56

11 MySQL Setup **57**

12 Todo List **58**

13 Namespace Documentation **59**

13.1 Package irbe_cli 59

13.1.1 Detailed Description 60

13.1.2 Function Documentation 61

13.1.3 Variable Documentation 61

13.2 Package irdbd 63

13.2.1 Detailed Description 64

13.2.2 Function Documentation 64

13.2.3 Variable Documentation 65

13.3 Package pubd 67

13.3.1 Detailed Description 68

13.3.2 Function Documentation 68

13.3.3 Variable Documentation 69

13.4 Package rootd 69

13.4.1 Detailed Description 70

13.4.2 Function Documentation 71

13.4.3 Variable Documentation 73

13.5 Package rpki 77

13.6 Package rpki.__doc__ 77

13.7 Package rpki.async 77

13.7.1 Detailed Description 78

13.7.2 Function Documentation 78

13.7.3 Variable Documentation 79

13.8 Package rpki.cli 80

13.8.1 Detailed Description 80

13.8.2 Function Documentation 80

13.8.3 Variable Documentation 81
13.9 Package rpki.config 81
13.9.1 Detailed Description 81
13.10 Package rpki.exceptions 82
13.10.1 Detailed Description 83
13.11 Package rpki.https 84
13.11.1 Detailed Description 85
13.11.2 Function Documentation 86
13.11.3 Variable Documentation 87
13.12 Package rpki.ipaddrs 89
13.12.1 Detailed Description 89
13.13 Package rpki.left_right 90
13.13.1 Detailed Description 90
13.13.2 Variable Documentation 91
13.14 Package rpki.log 91
13.14.1 Detailed Description 92
13.14.2 Function Documentation 92
13.14.3 Variable Documentation 93
13.15 Package rpki.manifest 94
13.15.1 Detailed Description 95
13.16 Package rpki.myrpki 95
13.16.1 Detailed Description 96
13.16.2 Function Documentation 97
13.16.3 Variable Documentation 98
13.17 Package rpki.oids 99
13.17.1 Detailed Description 99
13.17.2 Variable Documentation 100
13.18 Package rpki.publication 101
13.18.1 Detailed Description 101
13.19 Package rpki.relaxng 102
13.19.1 Variable Documentation 102

13.20 Package rpki.resource_set 103
13.20.1 Detailed Description 104
13.20.2 Function Documentation 104
13.20.3 Variable Documentation 105
13.21 Package rpki.roa 105
13.21.1 Detailed Description 106
13.22 Package rpki.rpki_engine 107
13.22.1 Detailed Description 107
13.23 Package rpki.sql 107
13.23.1 Detailed Description 108
13.24 Package rpki.sundial 108
13.24.1 Detailed Description 109
13.24.2 Function Documentation 109
13.25 Package rpki.up_down 110
13.25.1 Detailed Description 111
13.25.2 Variable Documentation 111
13.26 Package rpki.x509 112
13.26.1 Detailed Description 112
13.26.2 Function Documentation 113
13.27 Package rpki.xml_utils 114
13.27.1 Detailed Description 114
13.28 Package rpkid 114
13.28.1 Detailed Description 115
13.28.2 Function Documentation 115
13.28.3 Variable Documentation 116

14 Class Documentation **116**
14.1 async_chat Class Reference 116
14.2 dispatcher Class Reference 116
14.3 Cmd Class Reference 116
14.4 dict Class Reference 116

14.5 Exception Class Reference 117
14.6 irbe_cli.bsc_elt Class Reference 117
14.6.1 Detailed Description 119
14.6.2 Member Function Documentation 119
14.6.3 Member Data Documentation 120
14.7 irbe_cli.certificate_elt Class Reference 120
14.7.1 Detailed Description 121
14.8 irbe_cli.child_elt Class Reference 122
14.8.1 Detailed Description 124
14.9 irbe_cli.client_elt Class Reference 124
14.9.1 Detailed Description 126
14.10 irbe_cli.cmd_elt_mixin Class Reference 126
14.10.1 Detailed Description 128
14.10.2 Member Function Documentation 128
14.10.3 Member Data Documentation 130
14.11 irbe_cli.cmd_msg_mixin Class Reference 131
14.11.1 Detailed Description 132
14.11.2 Member Function Documentation 132
14.12 irbe_cli.config_elt Class Reference 132
14.12.1 Detailed Description 134
14.12.2 Member Function Documentation 134
14.12.3 Member Data Documentation 134
14.13 irbe_cli.crl_elt Class Reference 134
14.13.1 Detailed Description 135
14.14 irbe_cli.left_right_cms_msg Class Reference 136
14.14.1 Detailed Description 137
14.14.2 Member Data Documentation 137
14.15 irbe_cli.left_right_msg Class Reference 137
14.15.1 Detailed Description 139
14.15.2 Member Data Documentation 139
14.16 irbe_cli.left_right_proto Class Reference 139

14.16.1 Detailed Description 140
14.16.2 Member Data Documentation 140
14.17irbe_cli.left_right_sax_handler Class Reference 141
14.17.1 Detailed Description 142
14.17.2 Member Data Documentation 142
14.18irbe_cli.list_published_objects_elt Class Reference 142
14.18.1 Detailed Description 144
14.18.2 Member Data Documentation 144
14.19irbe_cli.list_received_resources_elt Class Reference 144
14.19.1 Detailed Description 146
14.19.2 Member Data Documentation 146
14.20irbe_cli.manifest_elt Class Reference 146
14.20.1 Detailed Description 147
14.21irbe_cli.parent_elt Class Reference 148
14.21.1 Detailed Description 150
14.22irbe_cli.publication_cms_msg Class Reference 150
14.22.1 Detailed Description 151
14.22.2 Member Data Documentation 152
14.23irbe_cli.publication_msg Class Reference 152
14.23.1 Detailed Description 154
14.23.2 Member Data Documentation 154
14.24irbe_cli.publication_proto Class Reference 154
14.24.1 Detailed Description 155
14.24.2 Member Data Documentation 155
14.25irbe_cli.publication_sax_handler Class Reference 156
14.25.1 Detailed Description 157
14.25.2 Member Data Documentation 157
14.26irbe_cli.reply_elt_mixin Class Reference 157
14.26.1 Detailed Description 158
14.26.2 Member Function Documentation 158
14.26.3 Member Data Documentation 159

14.27 irbe_cli.report_error_elt Class Reference 159
14.27.1 Detailed Description 160
14.28 irbe_cli.repository_elt Class Reference 160
14.28.1 Detailed Description 162
14.29 irbe_cli.roa_elt Class Reference 162
14.29.1 Detailed Description 163
14.30 irbe_cli.self_elt Class Reference 164
14.30.1 Detailed Description 166
14.31 irbe_cli.UsageWrapper Class Reference 166
14.31.1 Detailed Description 166
14.31.2 Member Function Documentation 167
14.32 long Class Reference 167
14.33 object Class Reference 167
14.34 pubd.pubd_context Class Reference 167
14.34.1 Detailed Description 169
14.34.2 Member Function Documentation 169
14.34.3 Member Data Documentation 170
14.35 datetime Class Reference 172
14.36 timedelta Class Reference 172
14.37 rootd.cms_msg Class Reference 172
14.37.1 Detailed Description 173
14.37.2 Member Data Documentation 174
14.38 rootd.issue_pdu Class Reference 174
14.38.1 Detailed Description 175
14.38.2 Member Function Documentation 176
14.39 rootd.list_pdu Class Reference 176
14.39.1 Detailed Description 177
14.39.2 Member Function Documentation 178
14.40 rootd.message_pdu Class Reference 178
14.40.1 Detailed Description 180
14.40.2 Member Function Documentation 180

14.40.3 Member Data Documentation 180
14.41 rootd.revoke_pdu Class Reference 181
14.41.1 Detailed Description 182
14.41.2 Member Function Documentation 182
14.42 rootd.sax_handler Class Reference 182
14.42.1 Detailed Description 183
14.42.2 Member Data Documentation 184
14.43 rpki.async.gc_summary Class Reference 184
14.43.1 Detailed Description 185
14.43.2 Member Function Documentation 185
14.43.3 Member Data Documentation 185
14.44 rpki.async.iterator Class Reference 186
14.44.1 Detailed Description 187
14.44.2 Member Function Documentation 187
14.44.3 Member Data Documentation 188
14.45 rpki.async.sync_wrapper Class Reference 189
14.45.1 Detailed Description 191
14.45.2 Member Function Documentation 191
14.45.3 Member Data Documentation 192
14.46 rpki.async.timer Class Reference 192
14.46.1 Detailed Description 194
14.46.2 Member Function Documentation 195
14.46.3 Member Data Documentation 197
14.47 rpki.cli.Cmd Class Reference 198
14.47.1 Detailed Description 200
14.47.2 Member Function Documentation 200
14.47.3 Member Data Documentation 202
14.48 rpki.config.parser Class Reference 203
14.48.1 Detailed Description 205
14.48.2 Member Function Documentation 205
14.48.3 Member Data Documentation 207

14.49 rpki.exceptions.BadClassNameSyntax Class Reference 208
14.49.1 Detailed Description 209
14.50 rpki.exceptions.BadClientURL Class Reference 209
14.50.1 Detailed Description 210
14.51 rpki.exceptions.BadContactURL Class Reference 210
14.51.1 Detailed Description 211
14.52 rpki.exceptions.BadExtension Class Reference 211
14.52.1 Detailed Description 212
14.53 rpki.exceptions.BadIRDBReply Class Reference 212
14.53.1 Detailed Description 213
14.54 rpki.exceptions.BadIssueResponse Class Reference 213
14.54.1 Detailed Description 214
14.55 rpki.exceptions.BadPKCS10 Class Reference 214
14.55.1 Detailed Description 215
14.56 rpki.exceptions.BadPublicationReply Class Reference 215
14.56.1 Detailed Description 216
14.57 rpki.exceptions.BadQuery Class Reference 216
14.57.1 Detailed Description 217
14.58 rpki.exceptions.BadSender Class Reference 217
14.58.1 Detailed Description 218
14.59 rpki.exceptions.BadStatusCode Class Reference 218
14.59.1 Detailed Description 219
14.60 rpki.exceptions.BadURISyntax Class Reference 219
14.60.1 Detailed Description 220
14.61 rpki.exceptions.BSCNotFound Class Reference 220
14.61.1 Detailed Description 221
14.62 rpki.exceptions.BSCNotReady Class Reference 221
14.62.1 Detailed Description 222
14.63 rpki.exceptions.ChildNotFound Class Reference 222
14.63.1 Detailed Description 223
14.64 rpki.exceptions.ClassNameMismatch Class Reference 223

14.64.1 Detailed Description 224
14.65 rpki.exceptions.ClassNameUnknown Class Reference 224
14.65.1 Detailed Description 225
14.66 rpki.exceptions.ClientNotFound Class Reference 225
14.66.1 Detailed Description 226
14.67 rpki.exceptions.CMSContentNotSet Class Reference 226
14.67.1 Detailed Description 227
14.68 rpki.exceptions.CMSCRLNotSet Class Reference 228
14.68.1 Detailed Description 228
14.69 rpki.exceptions.CMSVerificationFailed Class Reference 229
14.69.1 Detailed Description 229
14.70 rpki.exceptions.DBConsistancyError Class Reference 230
14.70.1 Detailed Description 230
14.71 rpki.exceptions.DERObjectConversionError Class Reference 231
14.71.1 Detailed Description 231
14.72 rpki.exceptions.DuplicateObject Class Reference 232
14.72.1 Detailed Description 232
14.73 rpki.exceptions.EmptyPEM Class Reference 233
14.73.1 Detailed Description 233
14.74 rpki.exceptions.EmptyROAPrefixList Class Reference 234
14.74.1 Detailed Description 234
14.75 rpki.exceptions.ForbiddenURI Class Reference 235
14.75.1 Detailed Description 235
14.76 rpki.exceptions.HandleTranslationError Class Reference 236
14.76.1 Detailed Description 236
14.77 rpki.exceptions.HTTPRequestFailed Class Reference 237
14.77.1 Detailed Description 237
14.78 rpki.exceptions.HTTPSBadVersion Class Reference 238
14.78.1 Detailed Description 238
14.79 rpki.exceptions.HTTPSClientAborted Class Reference 239
14.79.1 Detailed Description 239

14.80 rpki.exceptions.HTTPSUnexpectedState Class Reference 240
14.80.1 Detailed Description 240
14.81 rpki.exceptions.MissingCMSCRL Class Reference 241
14.81.1 Detailed Description 241
14.82 rpki.exceptions.MissingCMSEEcert Class Reference 242
14.82.1 Detailed Description 242
14.83 rpki.exceptions.MultipleTLSEECert Class Reference 243
14.83.1 Detailed Description 244
14.84 rpki.exceptions.MustBePrefix Class Reference 244
14.84.1 Detailed Description 245
14.85 rpki.exceptions.NoActiveCA Class Reference 245
14.85.1 Detailed Description 246
14.86 rpki.exceptions.NoCoveringCertForROA Class Reference 246
14.86.1 Detailed Description 247
14.87 rpki.exceptions.NoObjectAtURI Class Reference 247
14.87.1 Detailed Description 248
14.88 rpki.exceptions.NotACertificateChain Class Reference 248
14.88.1 Detailed Description 249
14.89 rpki.exceptions.NotFound Class Reference 249
14.89.1 Detailed Description 250
14.90 rpki.exceptions.NotImplementedYet Class Reference 250
14.90.1 Detailed Description 251
14.91 rpki.exceptions.NotInDatabase Class Reference 251
14.91.1 Detailed Description 252
14.92 rpki.exceptions.ReceivedTLSCACert Class Reference 252
14.92.1 Detailed Description 253
14.93 rpki.exceptions.RPKI_Exception Class Reference 254
14.93.1 Detailed Description 255
14.94 rpki.exceptions.ServerShuttingDown Class Reference 255
14.94.1 Detailed Description 256
14.95 rpki.exceptions.SKIMismatch Class Reference 256

14.95.1 Detailed Description 257
14.96 rpki.exceptions.SubprocessError Class Reference 257
14.96.1 Detailed Description 258
14.97 rpki.exceptions.TLSValidationError Class Reference 258
14.97.1 Detailed Description 259
14.98 rpki.exceptions.UnexpectedCMSCerts Class Reference 260
14.98.1 Detailed Description 260
14.99 rpki.exceptions.UnexpectedCMSCRLs Class Reference 261
14.99.1 Detailed Description 261
14.100 rpki.exceptions.UnparsableCMSDER Class Reference 262
14.100.1 Detailed Description 262
14.101 rpki.exceptions.UpstreamError Class Reference 263
14.101.1 Detailed Description 263
14.102 rpki.exceptions.WrongEContentType Class Reference 264
14.102.1 Detailed Description 264
14.103 rpki.https.caller Class Reference 265
14.103.1 Detailed Description 266
14.103.2 Member Function Documentation 266
14.103.3 Member Data Documentation 266
14.104 rpki.https.http_client Class Reference 267
14.104.1 Detailed Description 269
14.104.2 Member Function Documentation 269
14.104.3 Member Data Documentation 272
14.105 rpki.https.http_listener Class Reference 274
14.105.1 Detailed Description 275
14.105.2 Member Function Documentation 275
14.105.3 Member Data Documentation 276
14.106 rpki.https.http_message Class Reference 277
14.106.1 Detailed Description 278
14.106.2 Member Function Documentation 278
14.106.3 Member Data Documentation 280

14.107 rpki.https.http_queue Class Reference 280
14.107.1 Detailed Description 282
14.107.2 Member Function Documentation 282
14.107.3 Member Data Documentation 283
14.108 rpki.https.http_request Class Reference 284
14.108.1 Detailed Description 286
14.108.2 Member Function Documentation 286
14.108.3 Member Data Documentation 287
14.109 rpki.https.http_response Class Reference 287
14.109.1 Detailed Description 289
14.109.2 Member Function Documentation 289
14.109.3 Member Data Documentation 289
14.110 rpki.https.http_server Class Reference 290
14.110.1 Detailed Description 292
14.110.2 Member Function Documentation 292
14.110.3 Member Data Documentation 294
14.111 rpki.https.http_stream Class Reference 295
14.111.1 Detailed Description 297
14.111.2 Member Function Documentation 298
14.111.3 Member Data Documentation 303
14.112 rpki.ipaddrs.v4addr Class Reference 304
14.112.1 Detailed Description 305
14.112.2 Member Function Documentation 305
14.112.3 Member Data Documentation 306
14.113 rpki.ipaddrs.v6addr Class Reference 306
14.113.1 Detailed Description 307
14.113.2 Member Function Documentation 308
14.113.3 Member Data Documentation 308
14.114 rpki.left_right.bsc_elt Class Reference 309
14.114.1 Detailed Description 311
14.114.2 Member Function Documentation 311

14.114.3 Member Data Documentation 312
14.115 rpki.left_right.child_elt Class Reference 314
14.115.1 Detailed Description 316
14.115.2 Member Function Documentation 316
14.115.3 Member Data Documentation 318
14.116 rpki.left_right.cms_msg Class Reference 319
14.116.1 Detailed Description 321
14.116.2 Member Data Documentation 321
14.117 rpki.left_right.data_elt Class Reference 321
14.117.1 Detailed Description 323
14.117.2 Member Function Documentation 323
14.117.3 Member Data Documentation 325
14.118 rpki.left_right.left_right_namespace Class Reference 325
14.118.1 Detailed Description 326
14.118.2 Member Data Documentation 326
14.119 rpki.left_right.list_published_objects_elt Class Reference 327
14.119.1 Detailed Description 329
14.119.2 Member Function Documentation 329
14.119.3 Member Data Documentation 330
14.120 rpki.left_right.list_received_resources_elt Class Reference 330
14.120.1 Detailed Description 332
14.120.2 Member Function Documentation 332
14.120.3 Member Data Documentation 332
14.121 rpki.left_right.list_resources_elt Class Reference 333
14.121.1 Detailed Description 335
14.121.2 Member Function Documentation 335
14.121.3 Member Data Documentation 336
14.122 rpki.left_right.list_roa_requests_elt Class Reference 337
14.122.1 Detailed Description 338
14.122.2 Member Function Documentation 338
14.122.3 Member Data Documentation 338

14.123 rpki.left_right.msg Class Reference 339
14.123.1 Detailed Description 341
14.123.2 Member Function Documentation 341
14.123.3 Member Data Documentation 341
14.124 rpki.left_right.parent_elt Class Reference 342
14.124.1 Detailed Description 344
14.124.2 Member Function Documentation 344
14.124.3 Member Data Documentation 346
14.125 rpki.left_right.report_error_elt Class Reference 348
14.125.1 Detailed Description 350
14.125.2 Member Function Documentation 350
14.125.3 Member Data Documentation 351
14.126 rpki.left_right.repository_elt Class Reference 352
14.126.1 Detailed Description 354
14.126.2 Member Function Documentation 354
14.126.3 Member Data Documentation 355
14.127 rpki.left_right.sax_handler Class Reference 356
14.127.1 Detailed Description 358
14.127.2 Member Data Documentation 358
14.128 rpki.left_right.self_elt Class Reference 358
14.128.1 Detailed Description 361
14.128.2 Member Function Documentation 361
14.128.3 Member Data Documentation 365
14.129 rpki.log.logger Class Reference 367
14.129.1 Detailed Description 368
14.129.2 Member Function Documentation 368
14.129.3 Member Data Documentation 368
14.130 rpki.manifest.FileAndHash Class Reference 369
14.130.1 Detailed Description 369
14.130.2 Member Function Documentation 370
14.130.3 Member Data Documentation 370

14.131 rpki.manifest.FilesAndHashes Class Reference 370
14.131.1 Detailed Description 371
14.131.2 Member Function Documentation 371
14.132 rpki.manifest.Manifest Class Reference 372
14.132.1 Detailed Description 373
14.132.2 Member Function Documentation 373
14.132.3 Member Data Documentation 373
14.133 rpki.myrpki.CA Class Reference 374
14.133.1 Detailed Description 376
14.133.2 Member Function Documentation 376
14.133.3 Member Data Documentation 379
14.134 rpki.myrpki.child Class Reference 381
14.134.1 Detailed Description 383
14.134.2 Member Function Documentation 383
14.134.3 Member Data Documentation 384
14.135 rpki.myrpki.children Class Reference 385
14.135.1 Detailed Description 386
14.135.2 Member Function Documentation 386
14.136 rpki.myrpki.comma_set Class Reference 387
14.136.1 Detailed Description 388
14.136.2 Member Function Documentation 388
14.137 rpki.myrpki.csv_reader Class Reference 389
14.137.1 Detailed Description 390
14.137.2 Member Function Documentation 390
14.137.3 Member Data Documentation 390
14.138 rpki.myrpki.EntityDB Class Reference 391
14.138.1 Detailed Description 392
14.138.2 Member Function Documentation 393
14.138.3 Member Data Documentation 393
14.139 rpki.myrpki.main Class Reference 393
14.139.1 Detailed Description 395

14.139.2 Member Function Documentation 395
14.139.3 Member Data Documentation 398
14.140 rpki.myrpki.parent Class Reference 400
14.140.1 Detailed Description 402
14.140.2 Member Function Documentation 402
14.140.3 Member Data Documentation 403
14.141 rpki.myrpki.parents Class Reference 403
14.141.1 Detailed Description 404
14.141.2 Member Function Documentation 404
14.142 rpki.myrpki.repositories Class Reference 405
14.142.1 Detailed Description 406
14.142.2 Member Function Documentation 406
14.143 rpki.myrpki.repository Class Reference 407
14.143.1 Detailed Description 408
14.143.2 Member Function Documentation 409
14.143.3 Member Data Documentation 409
14.144 rpki.myrpki.roa_request Class Reference 410
14.144.1 Detailed Description 412
14.144.2 Member Function Documentation 412
14.144.3 Member Data Documentation 413
14.145 rpki.myrpki.roa_requests Class Reference 414
14.145.1 Detailed Description 414
14.145.2 Member Function Documentation 414
14.146 rpki.publication.certificate_elt Class Reference 415
14.146.1 Detailed Description 417
14.146.2 Member Data Documentation 417
14.147 rpki.publication.client_elt Class Reference 417
14.147.1 Detailed Description 419
14.147.2 Member Function Documentation 419
14.147.3 Member Data Documentation 420
14.148 rpki.publication.cms_msg Class Reference 422

14.148.1 Detailed Description 424
14.148.2 Member Data Documentation 424
14.149 rpki.publication.config_elt Class Reference 424
14.149.1 Detailed Description 426
14.149.2 Member Function Documentation 426
14.149.3 Member Data Documentation 427
14.150 rpki.publication.control_elt Class Reference 428
14.150.1 Detailed Description 431
14.150.2 Member Function Documentation 431
14.151 rpki.publication.crl_elt Class Reference 431
14.151.1 Detailed Description 433
14.151.2 Member Data Documentation 433
14.152 rpki.publication.manifest_elt Class Reference 433
14.152.1 Detailed Description 435
14.152.2 Member Data Documentation 435
14.153 rpki.publication.msg Class Reference 435
14.153.1 Detailed Description 437
14.153.2 Member Function Documentation 437
14.153.3 Member Data Documentation 437
14.154 rpki.publication.publication_namespace Class Reference 438
14.154.1 Detailed Description 438
14.154.2 Member Data Documentation 439
14.155 rpki.publication.publication_object_elt Class Reference 439
14.155.1 Detailed Description 441
14.155.2 Member Function Documentation 441
14.155.3 Member Data Documentation 443
14.156 rpki.publication.report_error_elt Class Reference 444
14.156.1 Detailed Description 446
14.156.2 Member Function Documentation 446
14.156.3 Member Data Documentation 447
14.157 rpki.publication.roa_elt Class Reference 448

14.157.1 Detailed Description 450
14.157.2 Member Data Documentation 450
14.158 rpki.publication.sax_handler Class Reference 450
14.158.1 Detailed Description 452
14.158.2 Member Data Documentation 452
14.159 rpki.resource_set.resource_bag Class Reference 452
14.159.1 Detailed Description 454
14.159.2 Member Function Documentation 454
14.159.3 Member Data Documentation 456
14.160 rpki.resource_set.resource_range Class Reference 457
14.160.1 Detailed Description 458
14.160.2 Member Function Documentation 458
14.160.3 Member Data Documentation 458
14.161 rpki.resource_set.resource_range_as Class Reference 459
14.161.1 Detailed Description 460
14.161.2 Member Function Documentation 460
14.161.3 Member Data Documentation 460
14.162 rpki.resource_set.resource_range_ip Class Reference 461
14.162.1 Detailed Description 463
14.162.2 Member Function Documentation 463
14.163 rpki.resource_set.resource_range_ipv4 Class Reference 464
14.163.1 Detailed Description 466
14.163.2 Member Data Documentation 466
14.164 rpki.resource_set.resource_range_ipv6 Class Reference 466
14.164.1 Detailed Description 468
14.164.2 Member Data Documentation 468
14.165 rpki.resource_set.resource_set Class Reference 468
14.165.1 Detailed Description 470
14.165.2 Member Function Documentation 470
14.165.3 Member Data Documentation 472
14.166 rpki.resource_set.resource_set_as Class Reference 473

14.166.1 Detailed Description 474
14.166.2 Member Function Documentation 474
14.166.3 Member Data Documentation 475
14.167 rpki.resource_set.resource_set_ip Class Reference 475
14.167.1 Detailed Description 477
14.167.2 Member Function Documentation 477
14.167.3 Member Data Documentation 478
14.168 rpki.resource_set.resource_set_ipv4 Class Reference 478
14.168.1 Detailed Description 480
14.168.2 Member Data Documentation 480
14.169 rpki.resource_set.resource_set_ipv6 Class Reference 480
14.169.1 Detailed Description 482
14.169.2 Member Data Documentation 482
14.170 rpki.resource_set.roa_prefix Class Reference 482
14.170.1 Detailed Description 484
14.170.2 Member Function Documentation 484
14.170.3 Member Data Documentation 485
14.171 rpki.resource_set.roa_prefix_ipv4 Class Reference 486
14.171.1 Detailed Description 488
14.171.2 Member Data Documentation 488
14.172 rpki.resource_set.roa_prefix_ipv6 Class Reference 488
14.172.1 Detailed Description 490
14.172.2 Member Data Documentation 490
14.173 rpki.resource_set.roa_prefix_set Class Reference 490
14.173.1 Detailed Description 491
14.173.2 Member Function Documentation 492
14.174 rpki.resource_set.roa_prefix_set_ipv4 Class Reference 493
14.174.1 Detailed Description 495
14.174.2 Member Data Documentation 495
14.175 rpki.resource_set.roa_prefix_set_ipv6 Class Reference 495
14.175.1 Detailed Description 497

14.175.2 Member Data Documentation 497
14.176 rpki.roa.ROAIPAddress Class Reference 497
14.176.1 Detailed Description 498
14.176.2 Member Function Documentation 498
14.176.3 Member Data Documentation 499
14.177 rpki.roa.ROAIPAddresses Class Reference 499
14.177.1 Detailed Description 500
14.177.2 Member Function Documentation 500
14.178 rpki.roa.ROAIPAddressFamilies Class Reference 500
14.178.1 Detailed Description 501
14.178.2 Member Function Documentation 501
14.179 rpki.roa.ROAIPAddressFamily Class Reference 501
14.179.1 Detailed Description 502
14.179.2 Member Function Documentation 502
14.179.3 Member Data Documentation 503
14.180 rpki.roa.RouteOriginAttestation Class Reference 503
14.180.1 Detailed Description 504
14.180.2 Member Function Documentation 504
14.180.3 Member Data Documentation 504
14.181 rpki.rpki_engine.ca_detail_obj Class Reference 505
14.181.1 Detailed Description 507
14.181.2 Member Function Documentation 508
14.181.3 Member Data Documentation 512
14.182 rpki.rpki_engine.ca_obj Class Reference 514
14.182.1 Detailed Description 516
14.182.2 Member Function Documentation 516
14.182.3 Member Data Documentation 520
14.183 rpki.rpki_engine.child_cert_obj Class Reference 521
14.183.1 Detailed Description 523
14.183.2 Member Function Documentation 523
14.183.3 Member Data Documentation 525

14.184 rpki.rpki_engine.publication_queue Class Reference 526
14.184.1 Detailed Description 528
14.184.2 Member Function Documentation 528
14.184.3 Member Data Documentation 529
14.185 rpki.rpki_engine.revoked_cert_obj Class Reference 530
14.185.1 Detailed Description 531
14.185.2 Member Function Documentation 531
14.185.3 Member Data Documentation 532
14.186 rpki.rpki_engine.roa_obj Class Reference 533
14.186.1 Detailed Description 535
14.186.2 Member Function Documentation 535
14.186.3 Member Data Documentation 538
14.187 rpki.rpki_engine.rpkid_context Class Reference 540
14.187.1 Detailed Description 542
14.187.2 Member Function Documentation 543
14.187.3 Member Data Documentation 545
14.188 rpki.sql.session Class Reference 548
14.188.1 Detailed Description 549
14.188.2 Member Function Documentation 550
14.188.3 Member Data Documentation 551
14.189 rpki.sql.sql_persistent Class Reference 553
14.189.1 Detailed Description 555
14.189.2 Member Function Documentation 555
14.189.3 Member Data Documentation 559
14.190 rpki.sql.template Class Reference 560
14.190.1 Detailed Description 562
14.190.2 Member Function Documentation 562
14.190.3 Member Data Documentation 562
14.191 rpki.sundial.datetime Class Reference 563
14.191.1 Detailed Description 565
14.191.2 Member Function Documentation 565

14.191.3 Member Data Documentation 569
14.192 rpki.sundial.timedelta Class Reference 569
14.192.1 Detailed Description 571
14.192.2 Member Function Documentation 572
14.192.3 Member Data Documentation 574
14.193 rpki.up_down.base_elt Class Reference 575
14.193.1 Detailed Description 576
14.193.2 Member Function Documentation 576
14.194 rpki.up_down.certificate_elt Class Reference 577
14.194.1 Detailed Description 579
14.194.2 Member Function Documentation 579
14.194.3 Member Data Documentation 580
14.195 rpki.up_down.class_elt Class Reference 580
14.195.1 Detailed Description 582
14.195.2 Member Function Documentation 582
14.195.3 Member Data Documentation 583
14.196 rpki.up_down.class_response_syntax Class Reference 585
14.196.1 Detailed Description 586
14.196.2 Member Function Documentation 586
14.196.3 Member Data Documentation 587
14.197 rpki.up_down.cms_msg Class Reference 587
14.197.1 Detailed Description 589
14.197.2 Member Data Documentation 589
14.198 rpki.up_down.error_response_pdu Class Reference 589
14.198.1 Detailed Description 591
14.198.2 Member Function Documentation 591
14.198.3 Member Data Documentation 592
14.199 rpki.up_down.issue_pdu Class Reference 593
14.199.1 Detailed Description 595
14.199.2 Member Function Documentation 595
14.199.3 Member Data Documentation 596

14.200 pki.up_down.issue_response_pdu Class Reference 597
14.200.1 Detailed Description 598
14.200.2 Member Function Documentation 599
14.201 pki.up_down.list_pdu Class Reference 599
14.201.1 Detailed Description 601
14.201.2 Member Function Documentation 601
14.202 pki.up_down.list_response_pdu Class Reference 602
14.202.1 Detailed Description 602
14.203 pki.up_down.message_pdu Class Reference 603
14.203.1 Detailed Description 605
14.203.2 Member Function Documentation 605
14.203.3 Member Data Documentation 607
14.204 pki.up_down.multi_uri Class Reference 608
14.204.1 Detailed Description 609
14.204.2 Member Function Documentation 609
14.205 pki.up_down.revoke_pdu Class Reference 610
14.205.1 Detailed Description 612
14.205.2 Member Function Documentation 612
14.205.3 Member Data Documentation 613
14.206 pki.up_down.revoke_response_pdu Class Reference 613
14.206.1 Detailed Description 614
14.207 pki.up_down.revoke_syntax Class Reference 615
14.207.1 Detailed Description 616
14.207.2 Member Function Documentation 616
14.207.3 Member Data Documentation 616
14.208 pki.up_down.sax_handler Class Reference 617
14.208.1 Detailed Description 619
14.208.2 Member Data Documentation 619
14.209 pki.x509.CMS_object Class Reference 619
14.209.1 Detailed Description 622
14.209.2 Member Function Documentation 622

14.209.3 Member Data Documentation 623
14.210 pki.x509.CRL Class Reference 626
14.210.1 Detailed Description 627
14.210.2 Member Function Documentation 627
14.210.3 Member Data Documentation 629
14.211 pki.x509.DeadDrop Class Reference 630
14.211.1 Detailed Description 631
14.211.2 Member Function Documentation 631
14.211.3 Member Data Documentation 631
14.212 pki.x509.DER_CMS_object Class Reference 632
14.212.1 Detailed Description 633
14.212.2 Member Function Documentation 633
14.212.3 Member Data Documentation 633
14.213 pki.x509.DER_object Class Reference 634
14.213.1 Detailed Description 636
14.213.2 Member Function Documentation 636
14.213.3 Member Data Documentation 641
14.214 pki.x509.PEM_converter Class Reference 642
14.214.1 Detailed Description 643
14.214.2 Member Function Documentation 643
14.214.3 Member Data Documentation 644
14.215 pki.x509.PKCS10 Class Reference 644
14.215.1 Detailed Description 646
14.215.2 Member Function Documentation 646
14.215.3 Member Data Documentation 647
14.216 pki.x509.ROA Class Reference 648
14.216.1 Detailed Description 650
14.216.2 Member Function Documentation 650
14.216.3 Member Data Documentation 650
14.217 pki.x509.RSA Class Reference 651
14.217.1 Detailed Description 653

14.217.2 Member Function Documentation 653
14.217.3 Member Data Documentation 654
14.218 pki.x509.RSApublic Class Reference 655
14.218.1 Detailed Description 657
14.218.2 Member Function Documentation 657
14.218.3 Member Data Documentation 658
14.219 pki.x509.SignedManifest Class Reference 659
14.219.1 Detailed Description 660
14.219.2 Member Function Documentation 660
14.219.3 Member Data Documentation 661
14.220 pki.x509.X509 Class Reference 661
14.220.1 Detailed Description 663
14.220.2 Member Function Documentation 663
14.220.3 Member Data Documentation 666
14.221 pki.x509.XML_CMS_object Class Reference 667
14.221.1 Detailed Description 669
14.221.2 Member Function Documentation 669
14.221.3 Member Data Documentation 671
14.222 pki.xml_utils.base_elt Class Reference 671
14.222.1 Detailed Description 673
14.222.2 Member Function Documentation 673
14.222.3 Member Data Documentation 675
14.223 pki.xml_utils.data_elt Class Reference 676
14.223.1 Detailed Description 678
14.223.2 Member Function Documentation 678
14.224 pki.xml_utils.msg Class Reference 681
14.224.1 Detailed Description 683
14.224.2 Member Function Documentation 683
14.224.3 Member Data Documentation 684
14.225 pki.xml_utils.sax_handler Class Reference 685
14.225.1 Detailed Description 686

14.225.2 Member Function Documentation 686
14.225.3 Member Data Documentation 688
14.226 rpki.xml_utils.text_elt Class Reference 689
14.226.1 Detailed Description 690
14.226.2 Member Function Documentation 690
14.226.3 Member Data Documentation 690
14.227 Sequence Class Reference 691
14.228 SequenceOf Class Reference 691
14.229 Set Class Reference 691
14.230 TextWrapper Class Reference 691
14.231 ContentHandler Class Reference 692

15 File Documentation **692**
15.1 __doc__.py File Reference 692
15.1.1 Detailed Description 692
15.2 __init__.py File Reference 693
15.3 async.py File Reference 693
15.4 cli.py File Reference 694
15.5 config.py File Reference 694
15.6 exceptions.py File Reference 694
15.7 https.py File Reference 696
15.8 ipaddrs.py File Reference 697
15.9 irbe_cli.py File Reference 698
15.10 irdbd.py File Reference 699
15.11 left_right.py File Reference 700
15.12 log.py File Reference 700
15.13 manifest.py File Reference 701
15.14 myrpki.py File Reference 701
15.15 oids.py File Reference 702
15.16 pubd.py File Reference 703
15.17 publication.py File Reference 703

15.18relaxng.py File Reference 704
15.19resource_set.py File Reference 704
15.20roa.py File Reference 705
15.21rootd.py File Reference 706
15.22rpki_engine.py File Reference 707
15.23rpkid.py File Reference 708
15.24sql.py File Reference 708
15.25sundial.py File Reference 708
15.26up_down.py File Reference 709
15.27x509.py File Reference 709
15.28xml_utils.py File Reference 710

1 RPKI Engine Reference Manual

This collection of Python modules implements a prototype of the RPKI Engine. This is a work in progress.

See `http://viewvc.hactrn.net/subvert-rpki.hactrn.net/` for code and design documents.

The RPKI Engine is an implementation of the production-side tools for generating certificates, CRLs, and ROAs. The `relying party tools` are a separate (and much simpler) package.

The Subversion repository for the entire project is available for (read-only) anonymous access at `http://subvert-rpki.hactrn.net/`.

The documentation you're reading is generated automatically by Doxygen from comments and documentation in `the code`.

Besides the automatically-generated code documentation, this manual also includes documentation of the overall package:

- Overview of the tools
- Installation instructions
- MySQL setup instructions
- Configuration instructions

- The myrpki tool
- A description of the left-right protocol
- A description of the publication protocol
- A description of the BPKI model used to secure the up-down, left-right, and publication protocols
- A description of the several SQL database schemas
- Some suggestions for further reading

This work was funded from 2006 through 2008 by ARIN, in collaboration with the other Regional Internet Registries. Current work is funded by DHS.

2 Overview

2.1 Terminology

A few special terms that appear often enough in code or documentation that they need explaining.

Todo

These explanations should be fleshed out properly.

IRBE:

Internet Registry Back End.

IRDB:

Internet Registry Data Base.

BPKI:

Business PKI.

RPKI:

Resource PKI.

2.2 Programs

At present the package is intended to be run out of the `rpkid/` directory.

In addition to the library routines in the `rpkid/rpki/` directory, the package includes the following programs:

- `rpkid :` The main RPKI engine daemon.
- `pubd :` The publication engine daemon.
- `rootd` A separate daemon for handling the root of an RPKI certificate tree. This is essentially a stripped down version of rpkid with no SQL database, no left-right protocol implementation, and only the parent side of the up-down protocol. It's separate because the root is a special case in several ways and it was simpler to keep the special cases out of the main daemon.
- `irdbd :` A sample implementation of an IR database daemon. rpkid calls into this to perform lookups via the left-right protocol.
- `smoketest :` A test tool for running a collection of rpkid and irdb instances under common control, driven by a unified test script.
- `yamltest :` Another test tool which takes the same input format as `smoketest.py`, but with slightly different purpose. `smoketest.py` is intended to support regression tests, while `yamltest.py` is intended for automated testing of something closer to a real operational environment. There's a fair amount of code duplication between the two, and at some point they will probably be merged into a single program that supports both modes of operation.

Most of these programs take configuration files in a common format similar to that used by the OpenSSL command line tool. The test programs also take input in YAML format to drive the tests. Runs of the `yamltest` test tool will generate a fairly complete set configuration files which may be useful as examples.

Basic operation consists of creating the appropriate MySQL databases (see MySQL Setup), configuring relationships between parents and children and between publication clients and repositories (see The myrpki tool), starting `rpkid`, `pubd`, `rootd`, and `irdbd`, and using the left-right and publication control protocols (see The myrpki tool) to set up rpkid's and pubd's internal state. All other operations should occur either as a result of cron events or as a result of incoming left-right and up-down protocol requests.

The core programs are all event-driven, and are (in theory) capable of supporting an arbitrary number of hosted RPKI engines to run in a single rpkid instance, up to the performance limits of the underlying hardware.

At present the daemon programs all run in foreground, that is, the daemons themselves make no attempt to put themselves in background. The easiest way to run the servers is to run the `start_servers` script, which examines your `myrpki.conf` file and starts the appropriate servers in background using `myrpki.conf` as the configuration file for each server as well.

If you prefer, you can run each server by hand instead of using the script, eg, using Bourne shell syntax to run rpkid in background:

```
$ python rpkid.py &
$ echo >rpkid.pid  "$!"
```

All of the daemons use syslog by default. You can change this by running either the servers themselves or the `start_servers` script with the "-d" option. Used as an argument to a server directly, "-d" causes that server to log to `stderr` instead of to syslog. Used as an argument to `start_servers`, "-d" starts each of the servers with "-d" while redirecting `stderr` from each server to a separate log file. This is intended primarily for debugging.

Some of the options that the several daemons take are common to all daemons. Which daemon they affect depends only on which sections of which config files they are in. See Common Options for details.

2.3 rpkid

rpkid is the main RPKI engine daemon. Configuration of rpkid is a two step process: a config file to bootstrap rpkid to the point where it can speak using the left-right protocol, followed by dynamic configuration via the left-right protocol. The latter stage is handled by the `myrpki` tool.

rpkid stores dynamic data in an SQL database, which must have been created for it, as explained in the Installation Guide.

2.4 pubd

pubd is the publication daemon. It implements the server side of the publication protocol, and is used by rpkid to publish the certificates and other objects that rpkid generates.

pubd is separate from rpkid for two reasons:

- The hosting model allows entities which choose to run their own copies of rpkid to publish their output under a common publication point. In general, encouraging shared publication services where practical is a good thing for relying parties, as it will speed up rcynic synchronization time.

- The publication server has to run on (or at least close to) the publication point itself, which in turn must be on a publically reachable server to be useful. rpkid, on the other hand, need only be reachable by the IRBE and its children in the RPKI tree. rpkid is a much more complex piece of software than pubd, so in some situations it might make sense to wrap tighter firewall constraints around rpkid than would be practical if rpkid and pubd were a single program.

pubd stores dynamic data in an SQL database, which must have been created for it, as explained in the Installation Guide. pubd also stores the published objects themselves as disk files in a configurable location which should correspond to an appropriate module definition in rsync.conf; see the Configuration Guide for details.

2.5 rootd

rootd is a stripped down implmenetation of (only) the server side of the up-down protocol. It's a separate program because the root certificate of an RPKI certificate tree requires special handling and may also require a special handling policy. rootd is a simple implementation intended for test use, it's not suitable for use in a production system. All configuration comes via the config file; see the Configuration Guide for details.

2.6 irdbd

irdbd is a sample implemntation of the server side of the IRDB callback subset of the left-right protocol. In production use this service is a function of the IRBE stub; irdbd may be suitable for production use in simple cases, but an IR with a complex IRDB may need to extend or rewrite irdbd.

irdbd requires a pre-populated database to represent the IR's customers. irdbd expects this database to use the SQL schema defined in rpkid/irdbd.sql. Once this database has been populated, the IRBE stub needs to create the appropriate objects in rpkid's database via the control subset of the left-right protocol, and store the linkage handles (foreign keys into rpkid's database) in the IRDB. See the Installation Guide and the MySQL setup instructions for details.

2.7 smoketest

smoketest is a test harness to set up and run a collection of rpkid and irdbd instances under scripted control.

Unlike the programs described above, smoketest takes two configuration files in different languages. The first configuration file uses the same syntax as the above configuration files but is completely optional. The second configuration file is the test script, which is encoded using the YAML serialization language (see

http://www.yaml.org/ for more information on YAML). The YAML script is not optional, as it describes the test layout. smoketest is designed to support running a fairly wide set of test configurations as canned scripts without writing any new control code. The intent is to make it possible to write meaningful regression tests.

See smoketest.conf for what can go into the (optional) first configuration file.

See smoketest.yaml for what goes into the (required) second configuration file.

2.8 yamltest

yamltest is another test harness to set up and run a collection of rpkid and irdbd instances under scripted control. It is similar in many ways to smoketest , and in fact uses the same YAML test description language, but its purpose is different: smoketest runs a particular test scenario through a series of changes, then shuts it down; yamltest, on the other hand, sets up a test network using the same tools that a real user would (principally the myrpki tool), and leaves the test running indefinitely.

yamltest grew out of smoketest and the two probably should be merged back into a single tool which supports both kinds of testing.

3 Further Reading

If you're interested in this package you might also be interested in:

- The rcynic validation tool
- A live sample of rcynic's summary output

4 Installation Guide

Installation instructions for rpkid et al.

These are the production-side RPKI tools, for Internet Registries (RIRs, LIRs, etc). See the "rcynic" program for relying party tools.

rpkid is a set of Python modules supporting generation and maintenance of resource certificates. Most of the code is in the rpkid/rpki/ directory. rpkid itself is a relatively small program that calls the library modules. There are several other programs that make use of the same libraries, as well as a collection of test programs.

At present the package is intended to be run out of its build directory. Setting up proper installation in a system area using the Python distutils package would likely not be very hard but has not yet been done.

Note that initial development of this code has been on FreeBSD, so installation will probably be easiest on FreeBSD.

Before attempting to build the package, you need to install any missing prerequisites. Note that the Python code requires Python version 2.5 or 2.6. rpkid et al are mostly self-contained, but do require a small number of external packages to run.

- If your Python installation does not already include the sources files needed to compile new Python extension modules, you will need to install whatever package does include those source files. The need for and name of this package varies from system to system. On FreeBSD, the base Python interpreter package includes the development sources; on at least some Linux distributions, you have to install a separate "python-devel" package or something similar. If you get compilation errors trying to build the POW code (below) and the error message says something about the file "Python.h" being missing, this is almost certainly your problem.
- http://codespeak.net/lxml/, a Pythonic interface to the Gnome LibXML2 libraries. lxml in turn requires the LibXML2 C libraries.
  - FreeBSD: /usr/ports/devel/py-lxml
  - Fedora: python-lxml.i386
  - Ubuntu: python-lxml
- http://sourceforge.net/projects/mysql-python/, the Python "db" interface to MySQL. MySQLdb in turn requires MySQL client and server. rpkid et al have been tested with MySQL 5.0 and 5.1.
  - FreeBSD: /usr/ports/databases/py-MySQLdb
  - Fedora: MySQL-python.i386
  - Ubuntu: python-mysqldb

rpkid et al also make heavy use of a modified copy of the Python OpenSSL Wrappers (POW) package, but this copy has enough modifications and additions that it's included in the subversion tree.

The next step is to build the OpenSSL and POW binaries. At present the OpenSSL code is just a snapshot of the OpenSSL development sources, compiled with special options to enable RFC 3779 support that ISC wrote under previous contract to ARIN. The POW (Python OpenSSL Wrapper) library is an extended copy of the stock POW release.

To build these, cd to the top-level directory in the distribution and type "make".

```
$ cd $top
$ make
```

This should automatically build everything, in the right order, including staticly linking the POW extension module with the OpenSSL library to provide RFC 3779 support. If you get errors building POW, see the above discussion of Python development sources.

The architecture is intended to support hardware signing modules (HSMs), but the code to support them has not been written.

At this point, you should have all the necessary software installed to run the core programs, but you will probably want to test it. The test suite requires a few more external packages, only one of which is Python code.

- http://pyyaml.org/. Several of the test programs use PyYAML to parse a YAML description of a simulated allocation hierarchy to test.
  - FreeBSD: /usr/ports/devel/py-yaml
  - Ubuntu: python-yaml
- http://xmlsoft.org/XSLT/. Some of the test code uses xsltproc, from the Gnome LibXSLT package.
  - FreeBSD: /usr/ports/textproc/libxslt
  - Ubuntu: xsltproc

All tests should be run from the rpkid/ directories.

Some of the tests require MySQL databases to store their data. To set up all the databases that the tests will need, run the SQL commands in rpkid/smoketest.setup.sql. The MySQL command line client is usually the easiest way to do this, eg:

```
$ cd $top/rpkid
$ mysql -u root -p <smoketest.setup.sql
```

To run the tests, run "make all-tests":

```
$ cd $top/rpkid
$ make all-tests
```

If nothing explodes, your installation is probably ok. Any Python backtraces in the output indicate a problem.

There's a last set of tools that only developers should need, as they're only used when modifying schemas or regenerating the documentation. These tools are listed here for completeness.

- http://www.doxygen.org/. Doxygen in turn pulls in several other tools, notably Graphviz, pdfLaTeX, and Ghostscript.

  - FreeBSD: /usr/ports/devel/doxygen
  - Ubuntu: doxygen

- http://www.mbayer.de/html2text/. The documentation build process uses xsltproc and html2text to dump flat text versions of a few critical documentation pages.
  - FreeBSD: /usr/ports/textproc/html2text

- http://www.thaiopensource.com/relaxng/trang.html. Trang is used to convert RelaxNG schemas from the human-readable "compact" form to the XML form that LibXML2 understands. Trang in turn requires Java.
  - FreeBSD: /usr/ports/textproc/trang

- http://search.cpan.org/dist/SQL-Translator/. SQL-Translator, also known as "SQL Fairy", includes code to parse an SQL schema and dump a description of it as Graphviz input. SQL Fairy in turn requires Perl.
  - FreeBSD: /usr/ports/databases/p5-SQL-Translator

Once you've finished with installation, the next thing you should read is the Configuration Guide.

5 Configuration Guide

This section describes the configuration file syntax and settings.

Each of the programs that make up the RPKI tookit can potentially take its own configuration file, but for most uses this is unnecessarily complicated. The recommended approach is to use a single configuration file, and to put all of the parameters that a normal user might need to change into a single section of that configuration file, then reference these common settings from the program-specific sections of the configuration file via macro expansion. The configuration file parser supports a limited version of the macro facility used in OpenSSL's configuration parser. An expression such as

```
foo = ${bar::baz}
```

sets foo to the value of the `baz` variable from section `bar`. The section name `ENV` is special: it refers to environment variables.

5.1 myrpki.conf

The default name for the shared configuration file is `myrpki.conf`.

```
[myrpki]
```

The [myrpki] section of `myrpki.conf` contains all the parameters that you really need to configure.

```
# Handle naming hosted resource-holding entity (<self/>) represented
# by this myrpki instance.  Syntax is an identifier (ASCII letters,
# digits, hyphen, underscore -- no whitespace, non-ASCII characters,
# or other punctuation).  You need to set this.

handle                          = Me
```

Every resource-holding or server-operating entity needs a "handle", which is just an identifier by which the entity calls itself. Handles do not need to be globally unique, but should be chosen with an eye towards debugging operational problems: it's best if you use a handle that your parents and children will recognize as being you.

```
# Names of various files and directories.  Don't change these without
# a good reason.

roa_csv                         = roas.csv
prefix_csv                      = prefixes.csv
asn_csv                         = asns.csv
xml_filename                    = myrpki.xml
bpki_resources_directory        = bpki/resources
bpki_servers_directory          = bpki/servers
```

The myrpki tool requires filenames for several input data files, the "business PKI" databases used to secure CMS and TLS communications, and the XML intermediate format that it uses. Rather than hardwiring the names into the code, they're configured here. You can change the names if you must, but the defaults should be fine in most cases.

```
# Whether you want to run your own copy of rpkid (and irdbd).  You
# want this on unless somebody else is hosting rpkid service for you.

run_rpkid                       = true

# DNS hostname and server port numbers for rpkid and irdbd, if you're
# running them.  rpkid's server host has to be a publicly reachable
# name to be useful; irdbd's server host should always be localhost
# unless you really know what you are doing.  Port numbers can be any
# legal TCP port number that you're not using for something else.

rpkid_server_host               = rpkid.example.org
rpkid_server_port               = 4404
irdbd_server_host               = localhost
irdbd_server_port               = 4403
```

If you're hosting RPKI service for others, or are self-hosting, you want this on. If somebody else is running rpkid on your behalf and you're just shipping them your `myrpki.xml` file, you can turn this off.

If you're running rpkid at all, you'll need to set at least the rpkid_server_host parameter here. You may be able to use the default port numbers, or may need to pick different ones. Unless you plan to run irdbd on a different machine from rpkid, you should leave irdbd_server_host alone.

```
# Whether you want to run your own copy of pubd.  In general, it's
# best to use your parent's pubd if you can, to reduce the overall
# number of publication sites that relying parties need to check, so
# don't enable this unless you have a good reason.

run_pubd                        = false

# DNS hostname and server port number for pubd, if you're running it.
# Hostname has to be a publicly reachable name to be useful, port can
# be any legal TCP port number that you're not using for something
# else.

pubd_server_host                = pubd.example.org
pubd_server_port                = 4402

# Contact information to include in offers of repository service.
# This only matters when we're running pubd.  This should be a human
# readable string, perhaps containing an email address or URL.

pubd_contact_info               = repo-man@rpki.example.org
```

The myrpki tool will attempt to negotiate publication service for you with whatever publication service your parent is using, if you let it, so in most cases you should not need to run pubd unless you need to issue certificates for private IP address space or private Autononmous System Numbers.

If you do run pubd, you will need to set pubd_server_host. You may also need to set pubd_server_port, and you should provide something helpful as contact information in pubd_contact_info if you plan to offer publication service to your RPKI children, so that grandchildren (or descendents even further down the tree) who receive referrals to your service will know how to contact you.

```
# Whether you want to run your very own copy of rootd.  Don't enable
# this unless you really know what you're doing.

run_rootd                       = false

# Server port number for rootd, if you're running it.  This can be any
# legal TCP port number that you're not using for something else.

rootd_server_port               = 4401
```

You shouldn't run rootd unless you're the root of an RPKI tree. Who gets to be the root of the public RPKI tree is a political issue outside the scope of this document. For everybody else, the only reason for running rootd (other than test purposes) would

be to support certification of private IP addresses and ASNs. The core tools can do this without any problem, but the simplified configuration mechanism does not (yet) make this easy to do.

```
# Root of local directory tree where pubd (and rootd, sigh) should
# write out published data.  You need to configure this, and the
# configuration should match up with the directory where you point
# rsyncd.  Neither pubd nor rsyncd much cares -where- you tell them to
# put this stuff, the important thing is that the rsync:// URIs in
# generated certificates match up with the published objects so that
# relying parties can find and verify rpkid's published outputs.

publication_base_directory      = publication/

# rsyncd module name corresponding to publication_base_directory.
# This has to match the module you configured into rsyncd.conf.
# Leave this alone unless you have some need to change it.

publication_rsync_module        = rpki

# Hostname and optional port number for rsync:// URIs.  In most cases
# this should just be the same value as pubd_server_host.

publication_rsync_server        = ${myrpki::pubd_server_host}
```

These parameters control the mapping between the rsync URIs presented by `rsyncd` and the local filesystem on the machine where `pubd` and `rsyncd` run. Any changes here must also be reflected as changes in `rsyncd.conf`. In most cases you should not change the value of `publication_rsync_module` from the default; since pubd can't (and should not) rewrite `rsyncd.conf`, it's best to use a static rsync module name here and let `pubd` do its work underneath that name. In most cases `publication_rsync_server` should be the same as `publication_rsync_server`, which is what the macro invocation in the default setting does. `publication_base_directory`, like other pathnames in `myrpki.conf`, can be either a relative or absolute pathname; if relative, it's interpreted with respect to the directory in which the programs in question were started. In this specific case, it's probably better to use an absolute pathname, since this pathname must also appear in `rsyncd.conf`.

```
# SQL configuration.  You can ignore this if you're not running any of
# the daemons yourself.

# If you're comfortable with having all of the databases use the same
# MySQL username and password, set those values here.  It's ok to
# leave the default username alone, but you should use a locally
# generated password either here or in the individual settings below.

shared_sql_username             = rpki
shared_sql_password             = fnord

# If you want different usernames and passwords for the separate SQL
```

```
# databases, enter those settings here; the shared_sql_* settings are
# only referenced here, so you can remove them entirely if you're
# setting everything in this block.

rpkid_sql_database              = rpkid
rpkid_sql_username              = ${myrpki::shared_sql_username}
rpkid_sql_password              = ${myrpki::shared_sql_password}

irdbd_sql_database              = irdbd
irdbd_sql_username              = ${myrpki::shared_sql_username}
irdbd_sql_password              = ${myrpki::shared_sql_password}

pubd_sql_database               = pubd
pubd_sql_username               = ${myrpki::shared_sql_username}
pubd_sql_password               = ${myrpki::shared_sql_password}
```

These settings control how `rpkid`, `irdbd`, and `pubd` talk to the MySQL server. At minimum, each daemon needs its own database; in the simplest configuration, the username and password can be shared, which is what the macro references in the default configuration does. If for some reason you need to set different usernames and passwords for different daemons, you can do so by changing the daemon-specific variables.

```
# Name of OpenSSL binary.  You might need to change this if you have
# no system copy installed, or if the system copy doesn't support CMS.
# The copy of openssl built by this package should suffice.

openssl                         = openssl
```

The `myrpki` tool uses the `openssl` command line tool for most of its BPKI operations, for two reasons:

- To avoid duplicating CA-management functionality already provided by the command line tool, and
- To ease portability of the `myrpki` tool, so that a "hosted" resource holder can use it without needing to install entire toolkit.

The `myrpki` tool's use of OpenSSL does not require exotic features like RFC 3779 support, but it does require a version of the tool recent enough to support CMS and the `-ss_cert` argument to the `ca` command. Depending on the platform on which you are running this code, you may or may not have a system copy of the `openssl` tool installed that meets these criteria; if not, the `openssl` binary built when you compile the toolkit will suffice. This parameter allows you to tell `myrpki` where to find the binary, if necessary; the default just uses the system search path.

5.2 Other configuration files and options

In most cases the simplified configuration in the [myrpki] section of `myrpki.conf` should suffice, but in case you need to tinker, here are details on the the rest of the configuration options. In most cases the default name of the configuration file for a program is the name of the program followed by `".conf"`, and the section name is also named for the program, so that you can combine sections into a single configuration file as shown with `myrpki.conf`.

- Common configuration options
- rpkid configuration
- irdbd configuration
- pubd configuration
- rootd configuration
- configuration of the smoketest test harness
- test description language for the smoketest test harness

Once you've finished with configuration, the next thing you should read is the MySQL setup instructions.

5.3 Common Configuration Options

Some of the options that the several daemons take are common to all daemons.

Which daemon they affect depends only on which sections of which config files they are in.

The first group of options are debugging flags, which can be set to "true" or "false". If not specified, default values will be chosen (generally false).

`debug_http`:

Enable verbose http debug logging.

`debug_tls_certs`:

Enable verbose logging about tls certs.

`want_persistent_client:`

Enable http 1.1 persistence, client side.

`want_persistent_server:`

Enable http 1.1 persistence, server side.

`debug_cms_certs:`

Enable verbose logging about cms certs.

`sql_debug:`

Enable verbose logging about sql operations.

`gc_debug:`

Enable scary garbage collector debugging.

`timer_debug:`

Enable verbose logging of timer system.

There are also a few options that allow you to save CMS messages for audit or debugging. The save format is a simple MIME encoding in a Maildir-format mailbox. The current options are very crude, at some point we may provide finer grain controls.

`dump_outbound_cms:`

Dump messages we send to this mailbox.

`dump_inbound_cms:`

Dump messages we receive to this mailbox.

5.4 rpkid.conf

rpkid's default config file is rpkid.conf, start rpkid with "-c filename" to choose a different config file.

All options are in the section "[rpkid]". Certificates, keys, and trust anchors may be in either DER or PEM format.

Config file options:

`startup-message:`

String to log on startup, useful when debugging a collection of rpkid instances at once.

sql-username:

Username to hand to MySQL when connecting to rpkid's database.

sql-database:

MySQL's database name for rpkid's database.

sql-password:

Password to hand to MySQL when connecting to rpkid's database.

bpki-ta:

Name of file containing BPKI trust anchor. All BPKI certificate verification within rpkid traces back to this trust anchor.

rpkid-cert:

Name of file containing rpkid's own BPKI EE certificate.

rpkid-key:

Name of file containing RSA key corresponding to rpkid-cert.

irbe-cert:

Name of file containing BPKI certificate used by IRBE when talking to rpkid.

irdb-cert:

Name of file containing BPKI certificate used by irdbd.

irdb-url:

Service URL for irdbd. Must be a https:// URL.

server-host:

Hostname or IP address on which to listen for HTTPS connections. Current default is INADDR_ANY (IPv4 0.0.0.0); this will need to be hacked to support IPv6 for production.

server-port:

TCP port on which to listen for HTTPS connections.

5.5 irdbd.conf

irdbd's default config file is irdbd.conf, start irdbd with "-c filename" to choose a different config file.

All options are in the section "[irdbd]". Certificates, keys, and trust anchors may be in either DER or PEM format.

Config file options:

startup-message:

String to log on startup, useful when debugging a collection of irdbd instances at once.

sql-username:

Username to hand to MySQL when connecting to irdbd's database.

sql-database:

MySQL's database name for irdbd's database.

sql-password:

Password to hand to MySQL when connecting to irdbd's database.

bpki-ta:

Name of file containing BPKI trust anchor. All BPKI certificate validation in irdbd traces back to this trust anchor.

irdbd-cert:

Name of file containing irdbd's own BPKI certificate.

irdbd-key:

Name of file containing RSA key corresponding to irdbd-cert.

rpkid-cert:

Name of file containing certificate used the one and only by rpkid instance authorized to contact this irdbd instance.

https-url:

Service URL for irdbd. Must be a https:// URL.

5.6 pubd.conf

pubd's default config file is pubd.conf, start pubd with "-c filename" to choose a different config file.

All options are in the section "[pubd]". Certifiates, keys, and trust anchors may be either DER or PEM format.

Config file options:

sql-username:

Username to hand to MySQL when connecting to pubd's database.

sql-database:

MySQL's database name for pubd's database.

sql-password:

Password to hand to MySQL when connecting to pubd's database.

bpki-ta:

Name of file containing master BPKI trust anchor for pubd. All BPKI validation in pubd traces back to this trust anchor.

irbe-cert:

Name of file containing BPKI certificate used by IRBE when talking to pubd.

pubd-cert:

Name of file containing BPKI certificate used by pubd.

pubd-key:

Name of file containing RSA key corresponding to `pubd-cert`.

server-host:

Hostname or IP address on which to listen for HTTPS connections. Current default is INADDR_ANY (IPv4 0.0.0.0); this will need to be hacked to support IPv6 for production.

server-port:

TCP port on which to listen for HTTPS connections.

publication-base:

Path to base of filesystem tree where pubd should store publishable objects. Default is "publication/".

5.7 rootd.conf

rootd's default config file is rootd.conf, start rootd with "-c filename" to choose a different config file.

All options are in the section "[rootd]". Certificates, keys, and trust anchors may be in either DER or PEM format.

Config file options:

bpki-ta:

Name of file containing BPKI trust anchor. All BPKI certificate validation in rootd traces back to this trust anchor.

rootd-bpki-cert:

Name of file containing rootd's own BPKI certificate.

rootd-bpki-key:

Name of file containing RSA key corresponding to rootd-bpki-cert.

rootd-bpki-crl:

Name of file containing BPKI CRL that would cover rootd-bpki-cert had it been revoked.

child-bpki-cert:

Name of file containing BPKI certificate for rootd's one and only child (RPKI engine to which rootd issues an RPKI certificate).

server-host:

Hostname or IP address on which to listen for HTTPS connections. Default is localhost.

server-port:

TCP port on which to listen for HTTPS connections.

rpki-root-key:

Name of file containing RSA key to use in signing resource certificates.

rpki-root-cert:

Name of file containing self-signed root resource certificate corresponding to rpki-root-key.

rpki-root-dir:

Name of directory where rootd should write RPKI subject certificate, manifest, and CRL.

rpki-subject-cert:

Name of file that rootd should use to save the one and only certificate it issues. Default is "Subroot.cer".

rpki-root-crl:

Name of file to which rootd should save its RPKI CRL. Default is "Root.crl".

rpki-root-manifest:

Name of file to which rootd should save its RPKI manifest. Default is "Root.mnf".

rpki-subject-pkcs10:

Name of file that rootd should use when saving a copy of the received PKCS #10 request for a resource certificate. This is only used for debugging. Default is not to save the PKCS #10 request.

5.8 smoketest.conf

All of the options in smoketest's (optional) configuration file are overrides for wired-in default values.

In almost all cases the defaults will suffice. There are a ridiculous number of options, most of which noone will ever need, see the code for details. The default name for this configuration file is smoketest.conf, run smoketest with "-c filename" to change it.

5.9 smoketest.yaml

smoketest's second configuration file is named smoketest.yaml by default, run smoketest with "-y filename" to change it.

The YAML file contains multiple YAML "documents". The first document describes the initial test layout and resource allocations, subsequent documents describe modifications to the initial allocations and other parameters. Resources listed in the initial layout are aggregated automatically, so that a node in the resource hierarchy automatically receives the resources it needs to issue whatever its children are listed as holding. Actions in the subsequent documents are modifications to the current resource set, modifications to validity dates or other non-resource parameters, or special commands like "sleep".

Here's an example of current usage:

```
name:           Alice
valid_for:      2d
sia_base:       "rsync://alice.example/rpki/"
kids:
  - name: Bob
 kids:
   - name: Carol
     ipv4: 192.0.2.1-192.0.2.33
     asn:  64533
---
- name: Carol
  valid_add:   10
---
- name: Carol
  add_as: 33
  valid_add:   2d
---
- name: Carol
  valid_sub:   2d
---
- name: Carol
  valid_for:   10d
```

This specifies an initial layout consisting of an RPKI engine named "Alice", with one child "Bob", which in turn has one child "Carol". Carol has a set of assigned resources, and all resources in the system are initially set to be valid for two days from the time at which the test is started. The first subsequent document adds ten seconds to the validity interval for Carol's resources and makes no other modifications. The second subsequent document grants Carol additional resources and adds another two days to the validity interval for Carol's resources. The next document subtracts two days from the validity interval for Carol's resources. The final document sets the validity interval for Carol's resources to ten days.

Operators in subsequent (update) documents:

add_as:

Add ASN resources.

add_v4:

Add IPv4 resources.

add_v6:

Add IPv6 resources.

sub_as:

Subtract ASN resources.

sub_v4:

Subtract IPv4 resources.

`sub_v6`:

Subtract IPv6 resources.

`valid_until`:

Set an absolute expiration date.

`valid_for`:

Set a relative expiration date.

`valid_add`:

Add to validity interval.

`valid_sub`:

Subtract from validity interval.

`sleep` [interval]:

Sleep for specified interval, or until smoketest receives a SIGALRM signal.

`shell` cmd...:

Pass rest of line verbatim to /bin/sh and block until the shell returns.

Absolute timestamps should be in the form shown (UTC timestamp format as used in XML).

Intervals (`valid_add`, `valid_sub`, `valid_for`, `sleep`) are either integers, in which case they're interpreted as seconds, or are a string of the form "wD xH yM zS" where w, x, y, and z are integers and D, H, M, and S indicate days, hours, minutes, and seconds. In the latter case all of the fields are optional, but at least one must be specified. For example, "3D4H" means "three days plus four hours".

6 Left-Right Protocol

The left-right protocol is really two separate client/server protocols over separate channels between the RPKI engine and the IR back end (IRBE).

The IRBE is the client for one of the subprotocols, the RPKI engine is the client for the other.

6.1 initiated by the IRBE

This part of the protcol uses a kind of message-passing. Each object that the RPKI engine knows about takes five messages: "create", "set", "get", "list", and "destroy".

Actions which are not just data operations on objects are handled via an SNMP-like mechanism, as if they were fields to be set. For example, to generate a keypair one "sets" the "generate-keypair" field of a BSC object, even though there is no such field in the object itself as stored in SQL. This is a bit of a kludge, but the reason for doing it as if these were variables being set is to allow composite operations such as creating a BSC, populating all of its data fields, and generating a keypair, all as a single operation. With this model, that's trivial, otherwise it's at least two round trips.

Fields can be set in either "create" or "set" operations, the difference just being whether the object already exists. A "get" operation returns all visible fields of the object. A "list" operation returns a list containing what "get" would have returned on each of those objects.

Left-right protocol objects are encoded as signed CMS messages containing XML as eContent and using an eContentType OID of `id-ct-xml` (1.2.840.113549.1.9.16.1.28). These CMS messages are in turn passed as the data for HTTPS POST operations, with an HTTP content type of "application/x-rpki" for both the POST data and the response data.

All operations allow an optional "tag" attribute which can be any alphanumeric token. The main purpose of the tag attribute is to allow batching of multiple requests into a single PDU.

6.1.1 <self/> object

A `<self/>` object represents one virtual RPKI engine. In simple cases where the RPKI engine operator operates the engine only on their own behalf, there will only be one `<self/>` object, representing the engine operator's organization, but in environments where the engine operator hosts other entities, there will be one `<self/> object` per hosted entity (probably including the engine operator's own organization, considered as a hosted customer of itself).

Some of the RPKI engine's configured parameters and data are shared by all hosted entities, but most are tied to a specific `<self/>` object. Data which are shared by all hosted entities are referred to as "per-engine" data, data which are specific to a particular `<self/>` object are "per-self" data.

Since all other RPKI engine objects refer to a `<self/>` object via a "self_handle" value, one must create a `<self/>` object before one can usefully configure any other left-right protocol objects.

Every `<self/>` object has a self_handle attribute, which must be specified for the "create", "set", "get", and "destroy" actions.

Payload data which can be configured in a `<self/>` object:

`use_hsm` (attribute):

Whether to use a Hardware Signing Module. At present this option has no effect,

as the implementation does not yet support HSMs.

`crl_interval` (attribute):

Positive integer representing the planned lifetime of an RPKI CRL for this `<self/>`, measured in seconds.

`regen_margin` (attribute):

Positive integer representing how long before expiration of an RPKI certificiate a new one should be generated, measured in seconds. At present this only affects the one-off EE certificates associated with ROAs.

`bpki_cert` (element):

BPKI CA certificate for this `<self/>`. This is used as part of the certificate chain when validating incoming TLS and CMS messages, and should be the issuer of cross-certification BPKI certificates used in `<repository/>`, `<parent/>`, and `<child/>` objects. If the bpki_glue certificate is in use (below), the bpki_-cert certificate should be issued by the bpki_glue certificate; otherwise, the bpki_-cert certificate should be issued by the per-engine bpki_ta certificate.

`bpki_glue` (element):

Another BPKI CA certificate for this `<self/>`, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the bpki_glue certificate should be the issuer of the bpki_-cert certificate and should be issued by the per-engine bpki_ta certificate; if not needed, the bpki_glue certificate should be left unset.

Control attributes that can be set to "yes" to force actions:

`rekey`:

Start a key rollover for every RPKI CA associated with every `<parent/>` object associated with this `<self/>` object. This is the first phase of a key rollover operation.

`revoke`:

Revoke any remaining certificates for any expired key associated with any RPKI CA for any `<parent/>` object associated with this `<self/>` object. This is the second (cleanup) phase for a key rollover operation; it's separate from the first phase to leave time for new RPKI certificates to propegate and be installed.

`reissue`:

Not implemented, may be removed from protocol. Original theory was that this operation would force reissuance of any object with a changed key, but as that

happens automatically as part of the key rollover mechanism this operation seems unnecessary.

`run_now`:

Force immediate processing for all tasks associated with this <self/> object that would ordinarily be performed under cron. Not currently implemented.

`publish_world_now`:

Force (re)publication of every publishable object for this <self/> object. Not currently implemented. Intended to aid in recovery if RPKI engine and publication engine somehow get out of sync.

6.1.2 <bsc/> object

The <bsc/> ("business signing context") object represents all the BPKI data needed to sign outgoing CMS or HTTPS messages. Various other objects include pointers to a <bsc/> object. Whether a particular <self/> uses only one <bsc/> or multiple is a configuration decision based on external requirements: the RPKI engine code doesn't care, it just cares that, for any object representing a relationship for which it must sign messages, there be a <bsc/> object that it can use to produce that signature.

Every <bsc/> object has a bsc_handle, which must be specified for the "create", "get", "set", and "destroy" actions. Every <bsc/> also has a self_handle attribute which indicates the <self/> object with which this <bsc/> object is associated.

Payload data which can be configured in a <isc/> object:

`signing_cert` (element):

BPKI certificate to use when generating a signature.

`signing_cert_crl` (element):

CRL which would list signing_cert if it had been revoked.

Control attributes that can be set to "yes" to force actions:

`generate_keypair`:

Generate a new BPKI keypair and return a PKCS #10 certificate request. The resulting certificate, once issued, should be configured as this <bsc/> object's signing_cert.

Additional attributes which may be specified when specifying "generate_keypair":

`key_type`:

Type of BPKI keypair to generate. "rsa" is both the default and, at the moment, the only allowed value.

`hash_alg`:

Cryptographic hash algorithm to use with this keypair. "sha256" is both the default and, at the moment, the only allowed value.

`key_length`:

Length in bits of the keypair to be generated. "2048" is both the default and, at the moment, the only allowed value.

Replies to "create" and "set" actions that specify "generate-keypair" include a <bsc_-pkcs10/> element, as do replies to "get" and "list" actions for a `<bsc/>` object for which a "generate-keypair" command has been issued. The RPKI engine stores the PKCS #10 request, which allows the IRBE to reuse the request if and when it needs to reissue the corresponding BPKI signing certificate.

6.1.3 <parent/> object

The `<parent/>` object represents the RPKI engine's view of a particular parent of the current `<self/>` object in the up-down protocol. Due to the way that the resource hierarchy works, a given `<self/>` may obtain resources from multiple parents, but it will always have at least one; in the case of IANA or an RIR, the parent RPKI engine may be a trivial stub.

Every `<parent/>` object has a parent_handle, which must be specified for the "create", "get", "set", and "destroy" actions. Every `<parent/>` also has a self_handle attribute which indicates the `<self/>` object with which this `<parent/>` object is associated, a bsc_handle attribute indicating the `<bsc/>` object to be used when signing messages sent to this parent, and a repository_handle indicating the `<repository/>` object to be used when publishing issued by the certificate issued by this parent.

Payload data which can be configured in a `<parent/>` object:

`peer_contact_uri` (attribute):

HTTPS URI used to contact this parent.

`sia_base` (attribute):

The leading portion of an rsync URI that the RPKI engine should use when composing the publication URI for objects issued by the RPKI certificate issued by this parent.

`sender_name` (attribute):

Sender name to use in the up-down protocol when talking to this parent. The RPKI engine doesn't really care what this value is, but other implementations of the up-down protocol do care.

`recipient_name` (attribute):

Recipient name to use in the up-down protocol when talking to this parent. The RPKI engine doesn't really care what this value is, but other implementations of the up-down protocol do care.

`bpki_cms_cert` (element):

BPKI CMS CA certificate for this `<parent/>`. This is used as part of the certificate chain when validating incoming CMS messages If the bpki_cms_glue certificate is in use (below), the bpki_cms_cert certificate should be issued by the bpki_cms_glue certificate; otherwise, the bpki_cms_cert certificate should be issued by the bpki_cert certificate in the `<self/>` object.

`bpki_cms_glue` (element):

Another BPKI CMS CA certificate for this `<parent/>`, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the bpki_cms_glue certificate should be the issuer of the bpki_cms_cert certificate and should be issued by the bpki_cert certificate in the `<self/>` object; if not needed, the bpki_cms_glue certificate should be left unset.

`bpki_https_cert` (element):

BPKI HTTPS CA certificate for this `<parent/>`. This is like the bpki_cms_cert object, only used for validating incoming TLS messages rather than CMS.

`bpki_cms_glue` (element):

Another BPKI HTTPS CA certificate for this `<parent/>`, usually not needed. This is like the bpki_cms_glue certificate, only used for validating incoming TLS messages rather than CMS.

Control attributes that can be set to "yes" to force actions:

`rekey`:

This is like the rekey command in the `<self/>` object, but limited to RPKI CAs under this parent.

`reissue`:

This is like the reissue command in the `<self/>` object, but limited to RPKI CAs under this parent.

`revoke`:

This is like the revoke command in the <self/> object, but limited to RPKI CAs under this parent.

6.1.4 <child/> object

The <child/> object represents the RPKI engine's view of particular child of the current <self/> in the up-down protocol.

Every <child/> object has a child_handle, which must be specified for the "create", "get", "set", and "destroy" actions. Every <child/> also has a self_handle attribute which indicates the <self/> object with which this <child/> object is associated.

Payload data which can be configured in a <child/> object:

`bpki_cert` (element):

BPKI CA certificate for this <child/>. This is used as part of the certificate chain when validating incoming TLS and CMS messages. If the bpki_glue certificate is in use (below), the bpki_cert certificate should be issued by the bpki_glue certificate; otherwise, the bpki_cert certificate should be issued by the bpki_cert certificate in the <self/> object.

`bpki_glue` (element):

Another BPKI CA certificate for this <child/>, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the bpki_glue certificate should be the issuer of the bpki_cert certificate and should be issued by the bpki_cert certificate in the <self/> object; if not needed, the bpki_glue certificate should be left unset.

Control attributes that can be set to "yes" to force actions:

`reissue`:

Not implemented, may be removed from protocol.

6.1.5 <repository/> object

The <repository/> object represents the RPKI engine's view of a particular publication repository used by the current <self/> object.

Every <repository/> object has a repository_handle, which must be specified for the "create", "get", "set", and "destroy" actions. Every <repository/> also has a self_handle attribute which indicates the <self/> object with which this <repository/> object is associated.

Payload data which can be configured in a <repository/> object:

peer_contact_uri (attribute):

HTTPS URI used to contact this repository.

bpki_cms_cert (element):

BPKI CMS CA certificate for this <repository/>. This is used as part of the certificate chain when validating incoming CMS messages If the bpki_cms_-glue certificate is in use (below), the bpki_cms_cert certificate should be issued by the bpki_cms_glue certificate; otherwise, the bpki_cms_cert certificate should be issued by the bpki_cert certificate in the <self/> object.

bpki_cms_glue (element):

Another BPKI CMS CA certificate for this <repository/>, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the bpki_cms_glue certificate should be the issuer of the bpki_cms_cert certificate and should be issued by the bpki_cert certificate in the <self/> object; if not needed, the bpki_cms_glue certificate should be left unset.

bpki_https_cert (element):

BPKI HTTPS CA certificate for this <repository/>. This is like the bpki_-cms_cert object, only used for validating incoming TLS messages rather than CMS.

bpki_cms_glue (element):

Another BPKI HTTPS CA certificate for this <repository/>, usually not needed. This is like the bpki_cms_glue certificate, only used for validating incoming TLS messages rather than CMS.

At present there are no control attributes for <repository/> objects.

6.1.6 <route_origin/> object

This section is out-of-date. The <route_origin/> object has been replaced by the <list_roa_requests/> IRDB query, but the documentation for that hasn't been written yet.

The <route_origin/> object is a kind of prototype for a ROA. It contains all the information needed to generate a ROA once the RPKI engine obtains the appropriate RPKI certificates from its parent(s).

Note that a <route_origin/> object represents a ROA to be generated on behalf of <self/>, not on behalf of a <child/>. Thus, a hosted entity that has no children but which does need to generate ROAs would be represented by a hosted <self/> with no <child/> objects but one or more <route_origin/> objects. While lumping ROA generation in with the other RPKI engine activities may seem a little odd at first, it's a natural consequence of the design requirement that the RPKI daemon never transmit private keys across the network in any form; given this requirement, the RPKI engine that holds the private keys for an RPKI certificate must also be the engine which generates any ROAs that derive from that RPKI certificate.

The precise content of the <route_origin/> has changed over time as the underlying ROA specification has changed. The current implementation as of this writing matches what we expect to see in draft-ietf-sidr-roa-format-03, once it is issued. In particular, note that the exactMatch boolean from the -02 draft has been replaced by the prefix and maxLength encoding used in the -03 draft.

Payload data which can be configured in a <route_origin/> object:

asn (attribute):

Autonomous System Number (ASN) to place in the generated ROA. A single ROA can only grant authorization to a single ASN; multiple ASNs require multiple ROAs, thus multiple <route_origin/> objects.

ipv4 (attribute):

List of IPv4 prefix and maxLength values, see below for format.

ipv6 (attribute):

List of IPv6 prefix and maxLength values, see below for format.

Control attributes that can be set to "yes" to force actions:

suppress_publication:

Not implemented, may be removed from protocol.

The lists of IPv4 and IPv6 prefix and maxLength values are represented as comma-separated text strings, with no whitespace permitted. Each entry in such a string represents a single prefix/maxLength pair.

ABNF for these address lists:

```
<ROAIPAddress> ::= <address> "/" <prefixlen> [ "-" <max_prefixlen> ]
                       ; Where <max_prefixlen> defaults to the same
                       ; value as <prefixlen>.
```

```
<ROAIPAddressList> ::= <ROAIPAddress> *( "," <ROAIPAddress> )
```

For example, `"10.0.1.0/24-32,10.0.2.0/24"`, which is a shorthand form of `"10.0.1.0/24-32,10.0.2.0/24-24"`.

6.2 Operations initiated by the RPKI engine

The left-right protocol also includes queries from the RPKI engine back to the IRDB. These queries do not follow the message-passing pattern used in the IRBE-initiated part of the protocol. Instead, there's a single query back to the IRDB, with a corresponding response. The CMS and HTTPS encoding are the same as in the rest of the protocol, but the BPKI certificates will be different as the back-queries and responses form a separate communication channel.

6.2.1 <list_resources/> messages

The `<list_resources/>` query and response allow the RPKI engine to ask the IRDB for information about resources assigned to a particular child. The query must include both a `"self_handle"` attribute naming the `<self/>` that is making the request and also a `"child_handle"` attribute naming the child that is the subject of the query. The query and response also allow an optional `"tag"` attribute of the same form used elsewhere in this protocol, to allow batching.

A `<list_resources/>` response includes the following attributes, along with the `tag` (if specified), `self_handle`, and `child_handle` copied from the request:

`valid_until`:

A timestamp indicating the date and time at which certificates generated by the RPKI engine for these data should expire. The timestamp is expressed as an XML `xsd:dateTime`, must be expressed in UTC, and must carry the "Z" suffix indicating UTC.

`asn`:

A list of autonomous sequence numbers, expressed as a comma-separated sequence of decimal integers with no whitespace.

`ipv4`:

A list of IPv4 address prefixes and ranges, expressed as a comma-separated list of prefixes and ranges with no whitespace. See below for format details.

ipv6:

A list of IPv6 address prefixes and ranges, expressed as a comma-separated list of prefixes and ranges with no whitespace. See below for format details.

Entries in a list of address prefixes and ranges can be either prefixes, which are written in the usual address/prefixlen notation, or ranges, which are expressed as a pair of addresses denoting the beginning and end of the range, written in ascending order separated by a single "-" character. This format is superficially similar to the format used for prefix and maxLength values in the `<route_origin/>` object, but the semantics differ: note in particular that `<route_origin/>` objects don't allow ranges, while `<list_resources/>` messages don't allow a maxLength specification.

6.3 Error handling

Error in this protocol are handled at two levels.

Since all messages in this protocol are conveyed over HTTPS connections, basic errors are indicated via the HTTP response code. 4xx and 5xx responses indicate that something bad happened. Errors that make it impossible to decode a query or encode a response are handled in this way.

Where possible, errors will result in a `<report_error/>` message which takes the place of the expected protocol response message. `<report_error/>` messages are CMS-signed XML messages like the rest of this protocol, and thus can be archived to provide an audit trail.

`<report_error/>` messages only appear in replies, never in queries. The `<report_error/>` message can appear on either the "forward" (IRBE as client of RPKI engine) or "back" (RPKI engine as client of IRDB) communication channel.

The `<report_error/>` message includes an optional `"tag"` attribute to assist in matching the error with a particular query when using batching, and also includes a `"self_handle"` attribute indicating the `<self/>` that issued the error.

The error itself is conveyed in the `error_code` (attribute). The value of this attribute is a token indicating the specific error that occurred. At present this will be the name of a Python exception; the production version of this protocol will nail down the allowed error tokens here, probably in the RelaxNG schema.

The body of the `<report_error/>` element itself is an optional text string; if present, this is debugging information. At present this capabilty is not used, debugging information goes to syslog.

7 Publication protocol

The publication protocol is really two separate client/server protocols, between different parties.

The first is a configuration protocol for an IRBE to use to configure a publication engine, the second is the interface by which authorized clients request publication of specific objects.

Much of the architecture of the publication protocol is borrowed from the left-right protocol: like the left-right protocol, the publication protocol uses CMS-wrapped XML over HTTPS with the same eContentType OID and the same HTTPS content-type, and the overall style of the XML messages is very similar to the left-right protocol. All operations allow an optional "tag" attribute to allow batching.

The publication engine operates a single HTTPS server which serves both of these subprotocols. The two subprotocols share a single server port, but use distinct URLs to allow demultiplexing.

7.1 Publication control subprotocol

The control subprotocol reuses the message-passing design of the left-right protocol. Configured objects support the "create", "set", "get", "list", and "destroy" actions, or a subset thereof when the full set of actions doesn't make sense.

7.1.1 <config/> object

The <config/> object allows configuration of data that apply to the entire publication server rather than a particular client.

There is exactly one <config/> object in the publication server, and it only supports the "set" and "get" actions -- it cannot be created or destroyed.

Payload data which can be configured in a <config/> object:

`bpki_crl` (element):

This is the BPKI CRL used by the publication server when signing the CMS wrapper on responses in the publication subprotocol. As the CRL must be updated at regular intervals, it's not practical to restart the publication server when the BPKI CRL needs to be updated. The BPKI model doesn't require use of a BPKI CRL between the IRBE and the publication server, so we can use the publication control subprotocol to update the BPKI CRL.

7.1.2 <client/> object

The <client/> object represents one client authorized to use the publication server.

The <client/> object supports the full set of "create", "set", "get", "list", and "destroy" actions. Each client has a "client_handle" attribute, which is used in responses and must be specified in "create", "set", "get", or "destroy" actions.

Payload data which can be configured in a <client/> object:

`base_uri` (attribute):

This is the base URI below which this client is allowed to publish data. The publication server may impose additional constraints in the case of a child publishing beneath its parent.

`bpki_cert` (element):

BPKI CA certificate for this <client/>. This is used as part of the certificate chain when validating incoming TLS and CMS messages. If the bpki_glue certificate is in use (below), the bpki_cert certificate should be issued by the bpki_glue certificate; otherwise, the bpki_cert certificate should be issued by the publication engine's bpki_ta certificate.

`bpki_glue` (element):

Another BPKI CA certificate for this <client/>, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the bpki_glue certificate should be the issuer of the bpki_-cert certificate and should be issued by the publication engine's bpki_ta certificate; if not needed, the bpki_glue certificate should be left unset.

7.2 Publication subprotocol

The publication subprotocol is structured somewhat differently from the publication control protocol. Objects in the publication subprotocol represent objects to be published or objects to be withdrawn from publication. Each kind of object supports two actions: "publish" and "withdraw". In each case the XML element representing hte object to be published or withdrawn has a "uri" attribute which contains the publication URI. For "publish" actions, the XML element body contains the DER object to be published, encoded in Base64; for "withdraw" actions, the XML element body is empty.

In theory, the detailed access control for each kind of object might be different. In practice, as of this writing, access control for all objects is a simple check that the client's `"base_uri"` is a leading substring of the publication URI. Details of why access control might need to become more complicated are discussed in a later section.

7.2.1 <certificate/> object

The <certificate/> object represents an RPKI certificate to be published or withdrawn.

7.2.2 <crl/> object

The <crl/> object represents an RPKI CRL to be published or withdrawn.

7.2.3 <manifest/> object

The <manifest/> object represents an RPKI publication manifest to be published or withdrawn.

Note that part of the reason for the batching support in the publication protocol is because *every* publication or withdrawal action requires a new manifest, thus every publication or withdrawal action will involve at least two objects.

7.2.4 <roa/> object

The <roa/> object represents a ROA to be published or withdrawn.

7.3 Error handling

Error in this protocol are handled at two levels.

Since all messages in this protocol are conveyed over HTTPS connections, basic errors are indicated via the HTTP response code. 4xx and 5xx responses indicate that something bad happened. Errors that make it impossible to decode a query or encode a response are handled in this way.

Where possible, errors will result in a <report_error/> message which takes the place of the expected protocol response message. <report_error/> messages are CMS-signed XML messages like the rest of this protocol, and thus can be archived to provide an audit trail.

<report_error/> messages only appear in replies, never in queries. The <report_error/> message can appear in both the control and publication subprotocols.

The <report_error/> message includes an optional `"tag"` attribute to assist in matching the error with a particular query when using batching.

The error itself is conveyed in the `error_code` (attribute). The value of this attribute is a token indicating the specific error that occurred. At present this will be the name of a Python exception; the production version of this protocol will nail down the allowed error tokens here, probably in the RelaxNG schema.

The body of the <report_error/> element itself is an optional text string; if present, this is debugging information. At present this capabilty is not used, debugging information goes to syslog.

7.4 Additional access control considerations.

As detailed above, the publication protocol is trivially simple. This glosses over two bits of potential complexity:

- In the case where parent and child are sharing a repository, we'd like to nest child under parent, because testing has demonstrated that even on relatively slow hardware the delays involved in setting up separate rsync connections tend to dominate synchronization time for relying parties.

- The repository operator might also want to do some checks to assure itself that what it's about to allow the RPKI engine to publish is not dangerous toxic waste.

The up-down protocol includes a mechanism by which a parent can suggest a publication URI to each of its children. The children are not required to accept this hint, and the children must make separate arrangements with the repository operator (who might or might not be the same as the entity that hosts the children's RPKI engine operations) to use the suggested publication point, but if everything works out, this allows children to nest cleanly under their parents publication points, which helps reduce synchronization time for relying parties.

In this case, one could argue that the publication server is responsible for preventing one of its clients (the child in the above description) from stomping on data published by another of its clients (the parent in the above description). This goes beyond the basic access check and requires the publication server to determine whether the parent has given its consent for the child to publish under the parent. Since the RPKI certificate profile requires the child's publication point to be indicated in an SIA extension in a certificate issued by the parent to the child, the publication engine can infer this permission from the parent's issuance of a certificate to the child. Since, by definition, the parent also uses this publication server, this is an easy check, as the publication server should already have the parent's certificate available by the time it needs to check the child's certificate.

The previous paragraph only covers a "publish" action for a <certificate/> object. For "publish" actions on other objects, the publication server would need to trace permission back to the certificate issued by the parent; for "withdraw" actions, the publication server would have to perform the same checks it would perform for a "publish" action, using the current published data before withdrawing it. The latter in turn implies an ordering constraint on "withdraw" actions in order to preserve the data necessary for these access control decisions; as this may prove impractical, the publication server may probably need to make periodic sweeps over its published data looking for orphaned objects, but that's probably a good idea anyway.

Note that, in this publication model, any agreement that the repository makes to publish the RPKI engine's output is conditional upon the object to be published passing whatever access control checks the publication server imposes.

8 SQL database schemas

- rpkid database schema
- pubd database schema
- irdbd database schema

8.1 rpkid SQL schema

Figure 1: Diagram of rpkid.sql

```
-- $Id: rpkid.sql 2953 2010-01-15 02:50:16Z sra $

-- Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")
--
-- Permission to use, copy, modify, and distribute this software for any
-- purpose with or without fee is hereby granted, provided that the above
-- copyright notice and this permission notice appear in all copies.
--
-- THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
-- REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
-- AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
-- INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
-- LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
-- OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
-- PERFORMANCE OF THIS SOFTWARE.

-- Copyright (C) 2007-2008  American Registry for Internet Numbers ("ARIN")
--
-- Permission to use, copy, modify, and distribute this software for any
-- purpose with or without fee is hereby granted, provided that the above
-- copyright notice and this permission notice appear in all copies.
--
-- THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
-- REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
-- AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
-- INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
-- LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
-- OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
-- PERFORMANCE OF THIS SOFTWARE.

-- SQL objects needed by the RPKI engine (rpkid.py).

-- DROP TABLE commands must be in correct (reverse dependency) order
-- to satisfy FOREIGN KEY constraints.

DROP TABLE IF EXISTS roa_prefix;
DROP TABLE IF EXISTS roa;
DROP TABLE IF EXISTS revoked_cert;
DROP TABLE IF EXISTS child_cert;
DROP TABLE IF EXISTS child;
DROP TABLE IF EXISTS ca_detail;
DROP TABLE IF EXISTS ca;
DROP TABLE IF EXISTS parent;
DROP TABLE IF EXISTS repository;
DROP TABLE IF EXISTS bsc;
DROP TABLE IF EXISTS self;

CREATE TABLE self (
        self_id                 SERIAL NOT NULL,
        self_handle             VARCHAR(255) NOT NULL,
        use_hsm                 BOOLEAN NOT NULL DEFAULT FALSE,
        crl_interval            BIGINT UNSIGNED,
        regen_margin            BIGINT UNSIGNED,
        bpki_cert               LONGBLOB,
        bpki_glue               LONGBLOB,
        PRIMARY KEY             (self_id),
        UNIQUE                  (self_handle)
```

```
) ENGINE=InnoDB;

CREATE TABLE bsc (
        bsc_id                  SERIAL NOT NULL,
        bsc_handle              VARCHAR(255) NOT NULL,
        private_key_id          LONGBLOB,
        pkcs10_request          LONGBLOB,
        hash_alg                ENUM ('sha256'),
        signing_cert            LONGBLOB,
        signing_cert_crl        LONGBLOB,
        self_id                 BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (bsc_id),
        CONSTRAINT              bsc_self_id
        FOREIGN KEY             (self_id) REFERENCES self (self_id) ON DELETE CASCADE,
        UNIQUE                  (self_id, bsc_handle)
) ENGINE=InnoDB;

CREATE TABLE repository (
        repository_id           SERIAL NOT NULL,
        repository_handle       VARCHAR(255) NOT NULL,
        peer_contact_uri        TEXT,
        bpki_cert               LONGBLOB,
        bpki_glue               LONGBLOB,
        bsc_id                  BIGINT UNSIGNED NOT NULL,
        self_id                 BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (repository_id),
        CONSTRAINT              repository_self_id
        FOREIGN KEY             (self_id) REFERENCES self (self_id) ON DELETE CASCADE,
        CONSTRAINT              repository_bsc_id
        FOREIGN KEY             (bsc_id) REFERENCES bsc (bsc_id) ON DELETE CASCADE,
        UNIQUE                  (self_id, repository_handle)
) ENGINE=InnoDB;

CREATE TABLE parent (
        parent_id               SERIAL NOT NULL,
        parent_handle           VARCHAR(255) NOT NULL,
        bpki_cms_cert           LONGBLOB,
        bpki_cms_glue           LONGBLOB,
        bpki_https_cert         LONGBLOB,
        bpki_https_glue         LONGBLOB,
        peer_contact_uri        TEXT,
        sia_base                TEXT,
        sender_name             TEXT,
        recipient_name          TEXT,
        self_id                 BIGINT UNSIGNED NOT NULL,
        bsc_id                  BIGINT UNSIGNED NOT NULL,
        repository_id           BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (parent_id),
        CONSTRAINT              parent_repository_id
        FOREIGN KEY             (repository_id) REFERENCES repository (repository_id) ON DELETE CASC
        CONSTRAINT              parent_bsc_id
        FOREIGN KEY             (bsc_id) REFERENCES bsc (bsc_id) ON DELETE CASCADE,
        CONSTRAINT              parent_self_id
        FOREIGN KEY             (self_id) REFERENCES self (self_id) ON DELETE CASCADE,
        UNIQUE                  (self_id, parent_handle)
) ENGINE=InnoDB;
```

```
CREATE TABLE ca (
        ca_id                   SERIAL NOT NULL,
        last_crl_sn             BIGINT UNSIGNED NOT NULL,
        last_manifest_sn        BIGINT UNSIGNED NOT NULL,
        next_manifest_update    DATETIME,
        next_crl_update         DATETIME,
        last_issued_sn          BIGINT UNSIGNED NOT NULL,
        sia_uri                 TEXT,
        parent_resource_class   TEXT,
        parent_id               BIGINT UNSIGNED,
        PRIMARY KEY             (ca_id),
        CONSTRAINT              ca_parent_id
        FOREIGN KEY             (parent_id) REFERENCES parent (parent_id) ON DELETE CASCADE
) ENGINE=InnoDB;

CREATE TABLE ca_detail (
        ca_detail_id            SERIAL NOT NULL,
        public_key              LONGBLOB,
        private_key_id          LONGBLOB,
        latest_crl              LONGBLOB,
        crl_published           DATETIME,
        latest_ca_cert          LONGBLOB,
        manifest_private_key_id LONGBLOB,
        manifest_public_key     LONGBLOB,
        latest_manifest_cert    LONGBLOB,
        latest_manifest         LONGBLOB,
        manifest_published      DATETIME,
        state                   ENUM ('pending', 'active', 'deprecated', 'revoked') NOT NULL,
        ca_cert_uri             TEXT,
        ca_id                   BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (ca_detail_id),
        CONSTRAINT              ca_detail_ca_id
        FOREIGN KEY             (ca_id) REFERENCES ca (ca_id) ON DELETE CASCADE
) ENGINE=InnoDB;

CREATE TABLE child (
        child_id                SERIAL NOT NULL,
        child_handle            VARCHAR(255) NOT NULL,
        bpki_cert               LONGBLOB,
        bpki_glue               LONGBLOB,
        self_id                 BIGINT UNSIGNED NOT NULL,
        bsc_id                  BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (child_id),
        CONSTRAINT              child_bsc_id
        FOREIGN KEY             (bsc_id) REFERENCES bsc (bsc_id) ON DELETE CASCADE,
        CONSTRAINT              child_self_id
        FOREIGN KEY             (self_id) REFERENCES self (self_id) ON DELETE CASCADE,
        UNIQUE                  (self_id, child_handle)
) ENGINE=InnoDB;

CREATE TABLE child_cert (
        child_cert_id           SERIAL NOT NULL,
        cert                    LONGBLOB NOT NULL,
        published               DATETIME,
        ski                     TINYBLOB NOT NULL,
        child_id                BIGINT UNSIGNED NOT NULL,
        ca_detail_id            BIGINT UNSIGNED NOT NULL,
```

```
        PRIMARY KEY             (child_cert_id),
        CONSTRAINT              child_cert_ca_detail_id
        FOREIGN KEY             (ca_detail_id) REFERENCES ca_detail (ca_detail_id) ON DELETE CASCADE
        CONSTRAINT              child_cert_child_id
        FOREIGN KEY             (child_id) REFERENCES child (child_id) ON DELETE CASCADE
) ENGINE=InnoDB;

CREATE TABLE revoked_cert (
        revoked_cert_id         SERIAL NOT NULL,
        serial                  BIGINT UNSIGNED NOT NULL,
        revoked                 DATETIME NOT NULL,
        expires                 DATETIME NOT NULL,
        ca_detail_id            BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (revoked_cert_id),
        CONSTRAINT              revoked_cert_ca_detail_id
        FOREIGN KEY             (ca_detail_id) REFERENCES ca_detail (ca_detail_id) ON DELETE CASCADE
) ENGINE=InnoDB;

CREATE TABLE roa (
        roa_id                  SERIAL NOT NULL,
        asn                     BIGINT UNSIGNED,
        cert                    LONGBLOB,
        roa                     LONGBLOB,
        published               DATETIME,
        self_id                 BIGINT UNSIGNED NOT NULL,
        ca_detail_id            BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (roa_id),
        CONSTRAINT              roa_self_id
        FOREIGN KEY             (self_id) REFERENCES self (self_id) ON DELETE CASCADE,
        CONSTRAINT              roa_ca_detail_id
        FOREIGN KEY             (ca_detail_id) REFERENCES ca_detail (ca_detail_id) ON DELETE CASCADE
) ENGINE=InnoDB;

CREATE TABLE roa_prefix (
        prefix                  VARCHAR(40) NOT NULL,
        prefixlen               TINYINT UNSIGNED NOT NULL,
        max_prefixlen           TINYINT UNSIGNED NOT NULL,
        version                 TINYINT UNSIGNED NOT NULL,
        roa_id                  BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (roa_id, prefix, prefixlen, max_prefixlen),
        CONSTRAINT              roa_prefix_roa_id
        FOREIGN KEY             (roa_id) REFERENCES roa (roa_id) ON DELETE CASCADE
) ENGINE=InnoDB;

-- Local Variables:
-- indent-tabs-mode: nil
-- End:
```

8.2 pubd SQL Schema

Figure 2: Diagram of pubd.sql

```
-- $Id: pubd.sql 2953 2010-01-15 02:50:16Z sra $

-- Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")
--
-- Permission to use, copy, modify, and distribute this software for any
-- purpose with or without fee is hereby granted, provided that the above
-- copyright notice and this permission notice appear in all copies.
--
-- THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
-- REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
-- AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
-- INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
-- LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
-- OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
-- PERFORMANCE OF THIS SOFTWARE.

-- Copyright (C) 2008  American Registry for Internet Numbers ("ARIN")
--
-- Permission to use, copy, modify, and distribute this software for any
-- purpose with or without fee is hereby granted, provided that the above
-- copyright notice and this permission notice appear in all copies.
--
-- THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
-- REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
-- AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
-- INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
-- LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
-- OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
-- PERFORMANCE OF THIS SOFTWARE.

-- SQL objects needed by pubd.py.

-- The config table is weird because we're really only using it
-- to store one BPKI CRL, but putting this here lets us use a lot of
-- existing machinery and the alternatives are whacky in other ways.

DROP TABLE IF EXISTS client;
```

```
DROP TABLE IF EXISTS config;

CREATE TABLE config (
        config_id       SERIAL NOT NULL,
        bpki_crl        LONGBLOB,
        PRIMARY KEY     (config_id)
) ENGINE=InnoDB;

CREATE TABLE client (
        client_id       SERIAL NOT NULL,
        client_handle   VARCHAR(255) NOT NULL,
        base_uri        TEXT,
        bpki_cert       LONGBLOB,
        bpki_glue       LONGBLOB,
        PRIMARY KEY     (client_id),
        UNIQUE          (client_handle)
) ENGINE=InnoDB;

-- Local Variables:
-- indent-tabs-mode: nil
-- End:
```

8.3 irdbd SQL Schema

Figure 3: Diagram of irdbd.sql

```
-- $Id: irdbd.sql 2953 2010-01-15 02:50:16Z sra $

-- Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")
--
-- Permission to use, copy, modify, and distribute this software for any
-- purpose with or without fee is hereby granted, provided that the above
-- copyright notice and this permission notice appear in all copies.
--
-- THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
-- REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
```

```
-- AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
-- INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
-- LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
-- OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
-- PERFORMANCE OF THIS SOFTWARE.

-- Copyright (C) 2007-2008  American Registry for Internet Numbers ("ARIN")
--
-- Permission to use, copy, modify, and distribute this software for any
-- purpose with or without fee is hereby granted, provided that the above
-- copyright notice and this permission notice appear in all copies.
--
-- THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
-- REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
-- AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
-- INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
-- LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
-- OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
-- PERFORMANCE OF THIS SOFTWARE.

-- SQL objects needed by irdbd.py.  You only need this if you're using
-- irdbd.py as your IRDB; if you have a "real" backend you can do
-- anything you like so long as you implement the relevant portion of
-- the left-right protocol.

-- DROP TABLE commands must be in correct (reverse dependency) order
-- to satisfy FOREIGN KEY constraints.

DROP TABLE IF EXISTS roa_request_prefix;
DROP TABLE IF EXISTS roa_request;
DROP TABLE IF EXISTS registrant_net;
DROP TABLE IF EXISTS registrant_asn;
DROP TABLE IF EXISTS registrant;

CREATE TABLE registrant (
        registrant_id           SERIAL NOT NULL,
        registrant_handle       VARCHAR(255) NOT NULL,
        registrant_name         TEXT,
        registry_handle         VARCHAR(255),
        valid_until             DATETIME NOT NULL,
        PRIMARY KEY             (registrant_id),
        UNIQUE                  (registry_handle, registrant_handle)
) ENGINE=InnoDB;

CREATE TABLE registrant_asn (
        registrant_asn_id       SERIAL NOT NULL,
        start_as                BIGINT UNSIGNED NOT NULL,
        end_as                  BIGINT UNSIGNED NOT NULL,
        registrant_id           BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (registrant_asn_id),
        CONSTRAINT              registrant_asn_registrant_id
        FOREIGN KEY             (registrant_id) REFERENCES registrant (registrant_id) ON DELETE CASC
) ENGINE=InnoDB;

CREATE TABLE registrant_net (
        registrant_net_id       SERIAL NOT NULL,
        start_ip                VARCHAR(40) NOT NULL,
```

```
        end_ip                  VARCHAR(40) NOT NULL,
        version                 TINYINT UNSIGNED NOT NULL,
        registrant_id           BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (registrant_net_id),
        CONSTRAINT              registrant_net_registrant_id
        FOREIGN KEY             (registrant_id) REFERENCES registrant (registrant_id) ON DELETE CASC
) ENGINE=InnoDB;

CREATE TABLE roa_request (
        roa_request_id          SERIAL NOT NULL,
        roa_request_handle      VARCHAR(255) NOT NULL,
        asn                     BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (roa_request_id)
) ENGINE=InnoDB;

CREATE TABLE roa_request_prefix (
        prefix                  VARCHAR(40) NOT NULL,
        prefixlen               TINYINT UNSIGNED NOT NULL,
        max_prefixlen           TINYINT UNSIGNED NOT NULL,
        version                 TINYINT UNSIGNED NOT NULL,
        roa_request_id          BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY             (roa_request_id, prefix, prefixlen, max_prefixlen),
        CONSTRAINT              roa_request_prefix_roa_request_id
        FOREIGN KEY             (roa_request_id) REFERENCES roa_request (roa_request_id) ON DELETE C
) ENGINE=InnoDB;

-- Local Variables:
-- indent-tabs-mode: nil
-- End:
```

9 BPKI model

The "business PKI" (BPKI) is the PKI used to authenticate communication on the up-down, left-right, and publication protocols.

BPKI certificates are *not* resource PKI (RPKI) certificates. The BPKI is a separate PKI that represents relationships between the various entities involved in the production side of the RPKI system. In most cases the BPKI tree will follow existing business relationships, hence the "B" (Business) in "BPKI".

Setup of the BPKI is handled by the back end; for the most part, rpkid and pubd just use the result. The one place where the engines are directly involved in creation of new BPKI certificates is in the production of end-entity certificates for use by the engines.

For the most part an ordinary user of this package need not worry about the details explained here, as the myrpki tool takes care of all of this. However, users who want to understand what's going on behind the scenes or who have needs too complex for the myrpki tool to handle might want to understand the underlying model.

There are a few design principals that underly the chosen BPKI model:

- Each engine should rely on a single BPKI trust anchor which is controlled by

the back end entity that runs the engine; all other trust material should be cross-certified into the engine's BPKI tree.

- Private keys must never transit the network.
- Except for end entity certificates, the engine should only have access to the BPKI certificates; in particular, the private key for the BPKI trust anchor should not be accessible to the engine.
- The number of BPKI keys and certificates that the engine has to manage should be no larger than is necessary.

rpkid's hosting model adds an additional constraint: rpkid's BPKI trust anchor belongs to the entity operating rpkid, but the entities hosted by rpkid should have control of their own BPKI private keys. This implies the need for an additional layer of BPKI certificate hierarchy within rpkid.

Here is a simplified picture of what the BPKI might look like for an rpkid operator that hosts two entities, "Alice" and "Ellen":

Black objects belong to the hosting entity, blue objects belong to the hosted entities, red objects are cross-certified objects from the hosted entities' peers. The arrows indicate certificate issuance: solid arrows are the ones that rpkid will care about during certificate validation, dotted arrows show the origin of the EE certificates that rpkid uses to sign CMS and TLS messages.

There's one nasty bit where the model had to bend to fit the current state of the underlying protocols: it's not possible to use exactly the same BPKI keys and certificates for HTTPS and CMS. The reason for this is simple: each hosted entity has its own BPKI, as does the hosting entity, but the HTTPS listener is shared. The only ways to avoid sharing the HTTPS server certificate would be to use separate listeners for each hosted entity, which scales poorly, or to rely on the TLS "Server Name Indication" extension (RFC 4366 3.1) which is not yet widely implemented.

The certificate tree looks complicated, but the set of certificates needed to build any particular validation chain is obvious, again excepting the HTTPS server case, where the client certificate is the first hint that the engine has of the client's identity, so the server must be prepared to accept any current client certificate.

Detailed instructions on how to build a BPKI are beyond the scope of this document, but one can handle simple cases using the OpenSSL command line tool and cross_-certify; the latter is a tool designed specifically for the purpose of generating the cross-certification certificates needed to splice foreign trust material into a BPKI tree.

The BPKI tree for a pubd instance is similar to to the BPKI tree for an rpkid instance, but is a bit simpler, as pubd does not provide hosting in the same sense that rpkid does: pubd is a relatively simple server that publishes objects as instructed by its clients.

Here's a simplified picture of what the BPKI might look like for a pubd operator that serves two clients, "Alice" and "Bob":

While it is likely that RIRs (at least) will operate both rpkid and pubd instances, the two functions are conceptually separate. As far as pubd is concerned, it doesn't matter who operates the rpkid instance: pubd just has clients, each of which has trust material that has been cross-certified into pubd's BPKI. Similarly, rpkid doesn't really care who operates a pubd instance that it's been configured to use, it just treats that pubd as a foreign BPKI whose trust material has to be cross-certified into its own BPKI. Cross certification itself is done by the back end operator, using cross_certify or some equivalent tool; the resulting BPKI certificates are configured into rpkid and pubd via the left-right protocol and the control subprotocol of the publication protocol, respectively.

Because the BPKI tree is almost entirely controlled by the operating entity, CRLs are not necessary for most of the BPKI. The one exception to this is the EE certificates issued under the cross-certification points. These EE certificates are generated by the peer, not the local operator, and thus require CRLs. Because of this, both rpkid and pubd require regular updates of certain BPKI CRLs, again via the left-right and publication control protocols.

Because the left-right protocol and the publication control subprotocol are used to configure BPKI certificates and CRLs, they cannot themselves use certificates and CRLs configured in this way. This is why the configuration files for rpkid and pubd require static configuration of the left-right and publication control certificates.

10 The myrpki tool

The design of rpkid and friends assumes that certain tasks can be thrown over the wall to the registry's back end operation.

This was a deliberate design decision to allow rpkid et al to remain independent of existing database schema, business PKIs, and so forth that a registry might already have. All very nice, but it leaves someone who just wants to test the tools or who has no existing back end with a fairly large programming project. The `myrpki` tool attempts to fill that gap.

`myrpki` is a basic implementation of what a registry back end would need to use rpkid and friends. `myrpki` does not use every available option in the other programs, nor is it necessarily as efficient as possible. Large registries will almost certainly want to roll their own tools, perhaps using these as a starting point. Nevertheless, we hope that `myrpki` will at least provide a useful example, and may be adaquate for simple use.

`myrpki` is (currently) implemented as a single command line Python program. It has a number of commands, most of which are used for initial setup, some of which are used on an ongoing basis. `myrpki` can be run either in an interactive mode or by passing a single command on the command line when starting the program; the former mode is intended to be somewhat human-friendly, the latter mode is useful in scripting, cron jobs, and automated testing.

`myrpki` use has two distinct phases: setup and data maintenance. The setup phase is primarily about constructing the "business PKI" (BPKI) certificates that the daemons use to authenticate CMS and HTTPS messages and obtaining the service URLs needed to configure the daemons. The data maintenance phase is about configuring local data into the daemons.

`myrpki` uses the OpenSSL command line tool for almost all operations on keys and certificates; the one exception to this is the comamnd which talks directly to the daemons, as this command uses the same communication libraries as the daemons themselves do. The intent behind using the OpenSSL command line tool for everything else is to allow all the other commands to be run without requiring all the auxiliary packages upon which the daemons depend; this can be useful, eg, if one wants to run the back-end on a laptop while running the daemons on a server, in which case one might prefer not to have to install a bunch of unnecessary packages on the laptop.

During setup phase `myrpki` generates and processes small XML messages which it expects the user to ship to and from its parents, children, etc via some out-of-band means (email, perhaps with PGP signatures, USB stick, we really don't care). During data maintenance phase, `myrpki` does something similar with another XML file, to allow hosting of RPKI services; in the degenerate case where an entity is just self-hosting (ie, is running the daemons for itself, and only for itself), this latter XML file need not be sent anywhere.

The basic idea here is that a user who has resources maintains a set of .csv files containing a text representation of the data needed by the back-end, along with a configuration

file containing other parameters. The intent is that these be very simple files that are easy to generate either by hand or as a dump from relational database, spreadsheet, awk script, whatever works in your environment. Given these files, the user then runs `myrpki` to extract the relevant information and encode everything about its back end state into an XML file, which can then be shipped to the appropriate other party.

Many of the `myrpki` commands which process XML input write out a new XML file, either in place or as an entirely new file; in general, these files need to be sent back to the party that sent the original file. Think of all this as a very slow packet-based communication channel, where each XML file is a single packet. In setup phase, there's generally a single round-trip per setup conversation; in the data maintenance phase, the same XML file keeps bouncing back and forth between hosted entity and hosting entity.

Note that, as certificates and CRLs have expiration and nextUpdate values, a low-level cycle of updates passing between resource holder and rpkid operator will be necessary as a part of steady state operation. [The current version of these tools does not yet regenerate these expiring objects, but fixing this will be a relatively minor matter.]

The third important kind of file in this system is the configuration file for `myrpki`. This contains a number of sections, some of which are for myrpki, others of which are for the OpenSSL command line tool, still others of which are for the various RPKI daemon programs. The examples/ subdirectory contains a commented version of the configuration file that explains the various parameters.

The .csv files read by myrpki are (now) misnamed: formerly, they used the "excel-tab" format from the Python csv library, but early users kept trying to make the colums line up, which didn't do what the users expected. So now these files are just whitespace-delimted, such as a program like "awk" would understand.

Keep reading, and don't panic.

The default configuration file name for `myrpki` is `myrpki.conf`. You can change this using the "-c" option when invoking myrpki, or by setting the environment variable MYRPKI_CONF.

See examples/∗.csv for commented examples of the several CSV files. Note that the comments themselves are not legal CSV, they're just present to make it easier to understand the examples.

10.1 Getting Started -- Overview

Which process you need to follow depends on whether you are running rpkid yourself or will be hosted by somebody else. We call the first case "self-hosted", because the software treats running rpkid to handle resources that you yourself hold as if you are an rpkid operator who is hosting an entity that happens to be yourself.

"$top" in the following refers to wherever you put the subvert-rpki.hactrn.net code. Once we have autoconf and "make install" targets, this will be some system directory or

another; for now, it's wherever you checked out a copy of the code from the subversion repository or unpacked a tarball of the code.

Most of the setup process looks the same for any resource holder, regardless of whether they are self-hosting or not. The differences come in the data maintenence phase.

The steps needed during setup phase are:

- Write a configuration file (copy $top/rpkid/examples/myrpki.conf and edit as needed). You need to configure the [myrpki] section; in theory, the rest of the file should be ok as it is, at least for simple use. You also need to create (either by hand or by dumping from a database, spreadsheet, whatever) the CSV files describing prefixes and ASNs you want to allocate to your children and ROAs you want created.

- Initialization ("initialize" command). This creates the local BPKI and other data structures that can be constructed just based on local data such as the config file. Other than some internal data structures, the main output of this step is the "identity.xml" file, which is used as input to later stages.

In theory it should be safe to run the "initialize" command more than once, in practice this has not (yet) been tested.

- Send (email, USB stick, carrier pigeon) identity.xml to each of your parents. This tells each of your parents what you call yourself, and supplies each parent with a trust anchor for your resource-holding BPKI.

- Each of your parents runs the "configure_child" command, giving the identity.xml you supplied as input. This registers your data with the parent, including BPKI cross-registration, and generates a return message containing your parent's BPKI trust anchors, a service URL for contacting your parent via the "up-down" protocol, and (usually) either an offer of publication service (if your parent operates a repository) or a referral from your parent to whatever publication service your parent does use. Referrals include a CMS-signed authorization token that the repository operator can use to determine that your parent has given you permission to home underneath your parent in the publication tree.

- Each of your parents sends (...) back the response XML file generated by the "configure_child" command.

- You feed the response message you just got into myrpki using the "configure_parent" command. This registers the parent's information in your database, including BPKI cross-certification, and processes the repository offer or referral to generate a publication request message.

- You send (...) the publication request message to the repository. The `contact_info` element in the request message should (in theory) provide some clue as to where you should send this.

- The repository operator processes your request using myrpki's "configure_-publication_client" command. This registers your information, including BPKI cross-certification, and generates a response message containing the repository's BPKI trust anchor and service URL.

- Repository operator sends (...) the publication confirmation message back to you.

- You process the publication confirmation message using myrpki's "configure_-repository" command.

At this point you should, in theory, have established relationships, exchanged trust anchors, and obtained service URLs from all of your parents and repositories. The last setup step is establishing a relationship with your RPKI service host, if you're not self-hosted, but as this is really just the first message of an ongoing exchange with your host, it's handled by the data maintenance commands.

The two commands used in data maintenence phase are "configure_resources" and "configure_daemons". The first is used by the resource holder, the second is used by the host. In the self-hosted case, it is not necessary to run "configure_resources" at all, myrpki will run it for you automatically.

10.2 Getting started -- Hosted case

The basic steps involved in getting started for a resource holder who is being hosted by somebody else are:

- Run through steps listed in the overview section.

- Run the configure_resources command to generate myrpki.xml.

- Send myrpki.xml to the rpkid operator who will be hosting you.

- Wait for your rpkid operator to ship you back an updated XML file containing a PKCS #10 certificate request for the BPKI signing context (BSC) created by rpkid.

- Run configure_resources again with the XML file you just received, to issue the BSC certificate and update the XML file again to contain the newly issued BSC certificate.

- Send the updated XML file back to your rpkid operator.

At this point you're done with initial setup. You will need to run configure_resources again whenever you make any changes to your configuration file or CSV files.

Warning

Once myrpki knows how to update BPKI CRLs, you will also need to run configure_resources periodically to keep your BPKI CRLs up to date.

Any time you run configure_resources myrpki, you should send the updated XML file to your rpkid operator, who should send you a further updated XML file in response.

10.3 Getting started -- Self-hosted case

The first few steps involved in getting started for a self-hosted resource holder (that is, a resource holder that runs its own copy of rpkid) are the same as in the hosted case above; after that the process diverges.

The [current] steps are:

- Follow the basic installation instructions in the Installation Guide to build the RFC-3779-aware OpenSSL code and associated Python extension module.

- Run through steps listed in the overview section.

- Set up the MySQL databases that rpkid et al will use. The package includes a tool to do this for you, you can use that or do the job by hand. See MySQL database setup for details.

- If you are running your own publication repository (that is, if you are running pubd), you will also need to set up an rsyncd server or configure your existing one to serve pubd's output. There's a sample configuration file in $top/rpkid/examples/rsyncd.conf, but you may need to do something more complicated if you are already running rsyncd for other purposes. See the rsync(1) and rsyncd.conf(5) manual pages for more details.

- Start the daemons. You can use $top/rpkid/start-servers.py to do this, or write your own script. If you intend to run pubd, you should make sure that the directory you specified as publication_base_directory exists and is writable by the userid that will be running pubd, and should also make sure to start rsyncd.

- Run myrpki's configure_daemons command, twice, with no arguments. You need to run the command twice because myrpki has to ask rpkid to create a keypair and generate a certification request for the BSC. The first pass does this, the

second processes the certification request, issues the BSC, and loads the result into rpkid. [Yes, we could automate this somehow, if necessary.]

At this point, if everything went well, rpkid should be up, configured, and starting to obtain resource certificates from its parents, generate CRLs and manifests, and so forth. At this point you should go figure out how to use the relying party tool, rcynic: see $top/rcynic/README if you haven't already done so.

If and when you change your CSV files, you should run configure_daemons again to feed the changes into the daemons.

10.4 started -- Hosting case

If you are running rpkid not just for your own resources but also to host other resource holders (see hosted case above), your setup will be almost the same as in the self-hosted case (see self-hosted case, above), with one procedural change: you will need to tell `configure_daemons` to process the XML files produced by the resource holders you are hosting. You do this by specifying the names of all those XML files on as arguments to the `configure_daemons` command. So, if you are hosting two friends, Alice and Bob, then, everywhere the instructions for the self-hosted case say to run `configure_daemons` with no arguments, you will instead run it with the names of Alice's and Bob's XML files as arguments.

Note that `configure_daemons` sometimes modifies these XML files, in which case it will write them back to the same filenames. While it is possible to figure out the set of circumstances in which this will happen (at present, only when `myrpki` has to ask `rpkid` to create a new BSC keypair and PKCS #10 certificate request), it may be easiest just to ship back an updated copy of the XML file after every you run `configure_daemons`.

10.5 Getting Started -- "Pure" hosting case

In general we assume that anybody who bothers to run `rpkid` is also a resource holder, but the software does not insist on this.

Todo

Er, well, rpkid doesn't, but myrpki now does -- "pure" hosting was an unused feature that fell by the wayside while simplifying the user interface. It would be relatively straightforward to add it back if we ever need it for anything, but the mechanism it used to use no longer exists -- the old [myirbe] section of the config file has been collapsed into the [myrpki] section, so testing for existance of the [myrpki] section no longer works. So we'll need an explicit configuration option, no big deal, just not worth chasing now.

A (perhaps) plausible use for this capability would be if you are an rpkid-running resource holder who wants for some reason to keep the resource-holding side of your operation completely separate from the rpkid-running side of your operation. This is essentially the pure-hosting model, just with an internal hosted entity within a different part of your own organization.

10.6 Troubleshooting

If you run into trouble setting up this package, the first thing to do is categorize the kind of trouble you are having. If you've gotten far enough to be running the daemons, check their log files. If you're seeing Python exceptions, read the error messages. If you're getting TLS errors, check to make sure that you're using all the right BPKI certificates and service contact URLs.

TLS configuration errors are, unfortunately, notoriously difficult to debug, because connection failures due to misconfiguration happen early, deep in the guts of the OpenSSL TLS code, where there isn't enough application context available to provide useful error messages.

If you've completed the steps above, everything appears to have gone OK, but nothing seems to be happening, the first thing to do is check the logs to confirm that nothing is actively broken. `rpkid's` log should include messages telling you when it starts and finishes its internal "cron" cycle. It can take several cron cycles for resources to work their way down from your parent into a full set of certificates and ROAs, so have a little patience. `rpkid's` log should also include messages showing every time it contacts its parent(s) or attempts to publish anything.

`rcynic` in fully verbose mode provides a fairly detailed explanation of what it's doing and why objects that fail have failed.

You can use `rsync` (sic) to examine the contents of a publication repository one directory at a time, without attempting validation, by running rsync with just the URI of the directory on its command line:

```
$ rsync rsync://rpki.example.org/where/ever/
```

10.7 Known Issues

The lxml package provides a Python interface to the Gnome libxml2 and libxslt C libraries. This code has been quite stable for several years, but initial testing with lxml compiled and linked against a newer version of libxml2 ran into problems (specifically, gratuitous RelaxNG schema validation failures). libxml2 2.7.3 worked; libxml2 2.7.5 did not work on the test machine in question. Reverting to libxml2 2.7.3 fixed the problem. Rewriting the two lines of Python code that were triggering the lxml bug appears to have solved the problem, so the code now works properly with libxml 2.7.5,

but if you start seeing weird XML validation failures, it might be another variation of this lxml bug.

An earlier version of this code ran into problems with what appears to be an implementation restriction in the the GNU linker ("ld") on 64-bit hardware, resulting in obscure build failures. The workaround for this required use of shared libraries and is somewhat less portable than the original code, but without it the code simply would not build in 64-bit environments with the GNU tools. The current workaround appears to behave properly, but the workaround requires that the pathname to the RFC-3779-aware OpenSSL shared libraries be built into the _POW.so Python extension module. At the moment, in the absence of "make install" targets for the Python code and libraries, this means the build directory; eventually, once we're using autoconf and installation targets, this will be the installation directory. If necessary, you can override this by setting the LD_LIBRARY_PATH environment variable, see the ld.so man page for details. This is a relatively minor variation on the usual build issues for shared libraries, it's just annoying because shared libraries should not be needed here and would not be if not for this GNU linker issue.

11 MySQL Setup

You need to install MySQL and set up the relevant databases before starting `rpkid`, `irdbd`, or `pubd`.

See the Installation Guide for details on where to download MySQL and find documentation on installing it.

See the Configuration Guide for details on the configuration file settings the daemons will use to find and authenticate themselves to their respective databases.

Before you can (usefully) start any of the daemons, you will need to set up the MySQL databases they use. You can do this by hand, or you can use the `sql-setup.py` script, which prompts you for your MySQL root password then attempts to do everything else automatically using values from myrpki.conf.

Using the script is simple:

```
$ python sql-setup.py
Please enter your MySQL root password:
```

The script should tell you what databases it creates. You can use the -v option if you want to see more details about what it's doing.

If you'd prefer to do the SQL setup manually, perhaps because you have valuable data in other MySQL databases and you don't want to trust some random setup script with your MySQL root password, you'll need to use the MySQL command line tool, as follows:

```
$ mysql -u root -p

mysql> CREATE DATABASE irdb_database;
mysql> GRANT all ON irdb_database.* TO irdb_user@localhost IDENTIFIED BY 'irdb_password';
mysql> USE irdb_database;
mysql> SOURCE $top/rpkid/irdbd.sql;
mysql> CREATE DATABASE rpki_database;
mysql> GRANT all ON rpki_database.* TO rpki_user@localhost IDENTIFIED BY 'rpki_password';
mysql> USE rpki_database;
mysql> SOURCE $top/rpkid/rpkid.sql;
mysql> COMMIT;
mysql> quit
```

where `irdb_database`, `irdb_user`, `irdb_password`, `rpki_database`, `rpki_user`, and `rpki_password` match the values you used in your configuration file.

If you are running pubd and are doing manual SQL setup, you'll also have to do:

```
$ mysql -u root -p
mysql> CREATE DATABASE pubd_database;
mysql> GRANT all ON pubd_database.* TO pubd_user@localhost IDENTIFIED BY 'pubd_password';
mysql> USE pubd_database;
mysql> SOURCE $top/rpkid/pubd.sql;
mysql> COMMIT;
mysql> quit
```

where `pubd_database`, `pubd_user` `pubd_password` match the values you used in your configuration file.

Once you've finished configuring MySQL, the next thing you should read is the instructions for the myrpki tool.

12 Todo List

Page Overview These explanations should be fleshed out properly.

Page The myrpki tool Er, well, rpkid doesn't, but myrpki now does -- "pure" hosting was an unused feature that fell by the wayside while simplifying the user interface. It would be relatively straightforward to add it back if we ever need it for anything, but the mechanism it used to use no longer exists -- the old [myirbe] section of the config file has been collapsed into the [myrpki] section, so testing for existance of the [myrpki] section no longer works. So we'll need an explicit configuration option, no big deal, just not worth chasing now.

13 Namespace Documentation

13.1 Package irbe_cli

Classes

- class bsc_elt
- class certificate_elt
- class child_elt
- class client_elt
- class cmd_elt_mixin
- class cmd_msg_mixin
- class config_elt
- class crl_elt
- class left_right_cms_msg
- class left_right_msg
- class left_right_proto
- class left_right_sax_handler
- class list_published_objects_elt
- class list_received_resources_elt
- class manifest_elt
- class parent_elt
- class publication_cms_msg
- class publication_msg
- class publication_proto
- class publication_sax_handler
- class reply_elt_mixin
- class report_error_elt
- class repository_elt
- class roa_elt
- class self_elt
- class UsageWrapper

Functions

- def usage

Variables

- list argv = sys.argv[1:]
- tuple call_pubd
- tuple call_rpkid
- tuple cfg = rpki.config.parser(cfg_file, "irbe_cli")
- string cfg_file = "irbe.conf"
- pem_out = None
- q_msg = q_msg_left_right
- list q_msg_left_right = [ ]
- list q_msg_publication = [ ]
- list q_pdu = left_right_msg.pdus[argv[0]]
- list top_opts = ["config=", "help", "pem_out=", "quiet", "verbose"]
- tuple usage_fill = UsageWrapper(subsequent_indent = " " ∗ 4)
- verbose = True

13.1.1 Detailed Description

```
Command line IR back-end control program for rpkid and pubd.

$Id: irbe_cli.py 3107 2010-03-16 23:13:08Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

13.1.2 Function Documentation

13.1.2.1 def irbe_cli.usage (*code* = 1)

Definition at line 240 of file irbe_cli.py.

13.1.3 Variable Documentation

13.1.3.1 tuple irbe_cli::argv = sys.argv[1:]

Definition at line 259 of file irbe_cli.py.

13.1.3.2 tuple irbe_cli.call_pubd

Initial value:

```
rpki.async.sync_wrapper(rpki.https.caller(
    proto       = publication_proto,
    client_key  = rpki.x509.RSA( Auto_file = cfg.get("pubd-irbe-key")),
    client_cert = rpki.x509.X509(Auto_file = cfg.get("pubd-irbe-cert")),
    server_ta   = rpki.x509.X509(Auto_file = cfg.get("pubd-bpki-ta")),
    server_cert = rpki.x509.X509(Auto_file = cfg.get("pubd-cert")),
    url         = cfg.get("pubd-url")),
    debug       = verbose)
```

Definition at line 323 of file irbe_cli.py.

13.1.3.3 tuple irbe_cli.call_rpkid

Initial value:

```
rpki.async.sync_wrapper(rpki.https.caller(
    proto       = left_right_proto,
    client_key  = rpki.x509.RSA( Auto_file = cfg.get("rpkid-irbe-key")),
    client_cert = rpki.x509.X509(Auto_file = cfg.get("rpkid-irbe-cert")),
    server_ta   = rpki.x509.X509(Auto_file = cfg.get("rpkid-bpki-ta")),
    server_cert = rpki.x509.X509(Auto_file = cfg.get("rpkid-cert")),
    url         = cfg.get("rpkid-url"),
    debug       = verbose))
```

Definition at line 306 of file irbe_cli.py.

13.1.3.4 tuple irbe_cli.cfg = rpki.config.parser(cfg_file, "irbe_cli")

Definition at line 283 of file irbe_cli.py.

13.1.3.5 irbe_cli.cfg_file = "irbe.conf"

Definition at line 264 of file irbe_cli.py.

13.1.3.6 irbe_cli.pem_out = None

Definition at line 39 of file irbe_cli.py.

13.1.3.7 irbe_cli.q_msg = q_msg_left_right

Definition at line 291 of file irbe_cli.py.

13.1.3.8 list irbe_cli.q_msg_left_right = [ ]

Definition at line 285 of file irbe_cli.py.

13.1.3.9 list irbe_cli.q_msg_publication = [ ]

Definition at line 286 of file irbe_cli.py.

13.1.3.10 list irbe_cli::q_pdu = left_right_msg.pdus[argv[0]]

Definition at line 290 of file irbe_cli.py.

13.1.3.11 list irbe_cli.top_opts = ["config=", "help", "pem_out=", "quiet", "verbose"]

Definition at line 238 of file irbe_cli.py.

13.1.3.12 tuple irbe_cli.usage_fill = UsageWrapper(subsequent_indent = " " * 4)

Definition at line 50 of file irbe_cli.py.

13.1.3.13 irbe_cli.verbose = True

Definition at line 265 of file irbe_cli.py.

13.2 Package irdbd

Functions

- def handle_list_resources
- def handle_list_roa_requests
- def handler

Variables

- tuple bpki_ta = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))
- tuple cfg = rpki.config.parser(cfg_file, "irdbd")
- string cfg_file = "irdbd.conf"
- tuple client_ta = (bpki_ta, rpkid_cert)
- tuple cur = db.cursor()
- tuple db
- dictionary handle_dispatch
- tuple handlers = ((u.path, handler),)
- string host = "localhost"
- tuple irdbd_cert = rpki.x509.X509(Auto_file = cfg.get("irdbd-cert"))
- tuple irdbd_key = rpki.x509.RSA(Auto_file = cfg.get("irdbd-key"))
- int port = 443
- tuple rpkid_cert = rpki.x509.X509(Auto_file = cfg.get("rpkid-cert"))

- server_cert = irdbd_cert,
- tuple startup_msg = cfg.get("startup-message", "")
- tuple u = urlparse.urlparse(cfg.get("https-url"))

13.2.1 Detailed Description

```
IR database daemon.

Usage: python irdbd.py [ { -c | --config } configfile ] [ { -h | --help } ]

Default configuration file is irdbd.conf, override with --config option.

$Id: irdbd.py 2913 2009-12-28 20:55:38Z sra $

Copyright (C) 2009  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

13.2.2 Function Documentation

13.2.2.1 def irdbd.handle_list_resources (*q_pdu*, *r_msg*)

Definition at line 53 of file irdbd.py.

13.2.2.2 def irdbd.handle_list_roa_requests (*q_pdu*, *r_msg*)

Definition at line 90 of file irdbd.py.

13.2.2.3 def irdbd.handler (*query*, *path*, *cb*)

Definition at line 119 of file irdbd.py.

13.2.3 Variable Documentation

13.2.3.1 tuple irdbd.bpki_ta = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))

Definition at line 201 of file irdbd.py.

13.2.3.2 tuple irdbd.cfg = rpki.config.parser(cfg_file, "irdbd")

Definition at line 186 of file irdbd.py.

13.2.3.3 irdbd.cfg_file = "irdbd.conf"

Definition at line 170 of file irdbd.py.

13.2.3.4 tuple irdbd.client_ta = (bpki_ta, rpkid_cert)

Definition at line 217 of file irdbd.py.

13.2.3.5 tuple irdbd.cur = db.cursor()

Definition at line 198 of file irdbd.py.

13.2.3.6 tuple irdbd.db

Initial value:

```
MySQLdb.connect(user   = cfg.get("sql-username"),
                     db     = cfg.get("sql-database"),
                     passwd = cfg.get("sql-password"))
```

Definition at line 194 of file irdbd.py.

13.2.3.7 dictionary irdbd.handle_dispatch

Initial value:

```
{
  rpki.left_right.list_resources_elt : handle_list_resources,
  rpki.left_right.list_roa_requests_elt : handle_list_roa_requests }
```

Definition at line 115 of file irdbd.py.

13.2.3.8 tuple irdbd.handlers = ((u.path, handler),)

Definition at line 220 of file irdbd.py.

13.2.3.9 string irdbd.host = "localhost"

Definition at line 218 of file irdbd.py.

13.2.3.10 tuple irdbd.irdbd_cert = rpki.x509.X509(Auto_file = cfg.get("irdbd-cert"))

Definition at line 203 of file irdbd.py.

13.2.3.11 tuple irdbd.irdbd_key = rpki.x509.RSA(Auto_file = cfg.get("irdbd-key"))

Definition at line 204 of file irdbd.py.

13.2.3.12 int irdbd.port = 443

Definition at line 219 of file irdbd.py.

13.2.3.13 tuple irdbd.rpkid_cert = rpki.x509.X509(Auto_file = cfg.get("rpkid-cert"))

Definition at line 202 of file irdbd.py.

13.2.3.14 irdbd.server_cert = irdbd_cert,

Definition at line 216 of file irdbd.py.

13.2.3.15 tuple irdbd.startup_msg = cfg.get("startup-message", "")

Definition at line 188 of file irdbd.py.

13.2.3.16 tuple irdbd.u = urlparse.urlparse(cfg.get("https-url"))

Definition at line 206 of file irdbd.py.

13.3 Package pubd

Classes

- class pubd_context

Functions

- def main

Variables

- string cfg_file = "pubd.conf"
- profile = False

13.3.1 Detailed Description

```
RPKI publication engine.

Usage: python pubd.py [ { -c | --config } configfile ]
                    [ { -h | --help } ]
                    [ { -p | --profile } outputfile ]

Default configuration file is pubd.conf, override with --config option.

$Id: pubd.py 3107 2010-03-16 23:13:08Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

13.3.2 Function Documentation

13.3.2.1 def pubd.main ()

Definition at line 174 of file pubd.py.

13.3.3 Variable Documentation

13.3.3.1 pubd.cfg_file = "pubd.conf"

Definition at line 155 of file pubd.py.

13.3.3.2 pubd.profile = False

Definition at line 156 of file pubd.py.

13.4 Package rootd

Classes

- class cms_msg
- class issue_pdu
- class list_pdu
- class message_pdu
- class revoke_pdu
- class sax_handler

Functions

- def compose_response
- def del_subject_cert
- def del_subject_pkcs10
- def get_root_cert
- def get_subject_cert
- def get_subject_pkcs10
- def issue_subject_cert_maybe
- def root_newer_than_subject
- def set_subject_cert
- def set_subject_pkcs10
- def up_down_handler

Variables

- tuple bpki_ta = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))
- tuple cfg = rpki.config.parser(cfg_file, "rootd")
- string cfg_file = "rootd.conf"
- tuple child_bpki_cert = rpki.x509.X509(Auto_file = cfg.get("child-bpki-cert"))
- tuple client_ta = (bpki_ta, child_bpki_cert)
- handlers = up_down_handler)
- host = https_server_host,
- tuple https_server_host = cfg.get("server-host", "")
- tuple https_server_port = int(cfg.get("server-port"))
- port = https_server_port,
- tuple rootd_bpki_cert = rpki.x509.X509(Auto_file = cfg.get("rootd-bpki-cert"))
- tuple rootd_bpki_crl = rpki.x509.CRL(Auto_file = cfg.get("rootd-bpki-crl"))
- tuple rootd_bpki_key = rpki.x509.RSA(Auto_file = cfg.get("rootd-bpki-key"))
- tuple rpki_base_uri = cfg.get("rpki-base-uri", "rsync://" + rpki_class_name + ".invalid/")
- tuple rpki_class_name = cfg.get("rpki-class-name", "wombat")
- rpki_root_cert = None
- tuple rpki_root_cert_file = cfg.get("rpki-root-cert")
- tuple rpki_root_cert_uri = cfg.get("rpki-root-cert-uri", rpki_base_uri + "Root.cer")
- tuple rpki_root_crl = cfg.get("rpki-root-crl", "Root.crl")
- tuple rpki_root_dir = cfg.get("rpki-root-dir")
- tuple rpki_root_key = rpki.x509.RSA(Auto_file = cfg.get("rpki-root-key"))
- tuple rpki_root_manifest = cfg.get("rpki-root-manifest", "Root.mnf")
- tuple rpki_subject_cert = cfg.get("rpki-subject-cert", "Child.cer")
- tuple rpki_subject_lifetime = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-lifetime", "30d"))
- tuple rpki_subject_pkcs10 = cfg.get("rpki-subject-pkcs10", "Child.pkcs10")
- tuple rpki_subject_regen = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-regen", rpki_subject_lifetime.convert_to_seconds() / 2))
- server_cert = rootd_bpki_cert,

13.4.1 Detailed Description

```
Trivial RPKI up-down protocol root server, for testing.  Not suitable
for production use.  Overrides a bunch of method definitions from the
rpki.* classes in order to reuse as much code as possible.

Usage: python rootd.py [ { -c | --config } configfile ] [ { -h | --help } ]

Default configuration file is rootd.conf, override with --config option.

$Id: rootd.py 2913 2009-12-28 20:55:38Z sra $
```

Copyright (C) 2009 Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

13.4.2 Function Documentation

13.4.2.1 def rootd.compose_response (*r_msg*, *pkcs10* = `None`)

Definition at line 175 of file rootd.py.

13.4.2.2 def rootd.del_subject_cert ()

Definition at line 72 of file rootd.py.

13.4.2.3 def rootd.del_subject_pkcs10 ()

Definition at line 91 of file rootd.py.

13.4.2.4 def rootd.get_root_cert ()

Definition at line 48 of file rootd.py.

13.4.2.5 def rootd.get_subject_cert ()

Definition at line 56 of file rootd.py.

13.4.2.6 def rootd.get_subject_pkcs10 ()

Definition at line 77 of file rootd.py.

13.4.2.7 def rootd.issue_subject_cert_maybe (*new_pkcs10*)

Definition at line 98 of file rootd.py.

13.4.2.8 def rootd.root_newer_than_subject ()

Definition at line 53 of file rootd.py.

13.4.2.9 def rootd.set_subject_cert (*cert*)

Definition at line 65 of file rootd.py.

13.4.2.10 def rootd.set_subject_pkcs10 (*pkcs10*)

Definition at line 85 of file rootd.py.

13.4.2.11 def rootd.up_down_handler (*query*, *path*, *cb*)

Definition at line 238 of file rootd.py.

13.4.3 Variable Documentation

13.4.3.1 tuple rootd.bpki_ta = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))

Definition at line 288 of file rootd.py.

13.4.3.2 tuple rootd.cfg = rpki.config.parser(cfg_file, "rootd")

Definition at line 284 of file rootd.py.

13.4.3.3 rootd.cfg_file = "rootd.conf"

Definition at line 268 of file rootd.py.

13.4.3.4 tuple rootd.child_bpki_cert = rpki.x509.X509(Auto_file = cfg.get("child-bpki-cert"))

Definition at line 292 of file rootd.py.

13.4.3.5 tuple rootd.client_ta = (bpki_ta, child_bpki_cert)

Definition at line 316 of file rootd.py.

13.4.3.6 rootd.handlers = up_down_handler)

Definition at line 319 of file rootd.py.

13.4.3.7 rootd.host = https_server_host,

Definition at line 317 of file rootd.py.

13.4.3.8 tuple rootd.https_server_host = cfg.get("server-host", "")

Definition at line 294 of file rootd.py.

13.4.3.9 tuple rootd.https_server_port = int(cfg.get("server-port"))

Definition at line 295 of file rootd.py.

13.4.3.10 rootd.port = https_server_port,

Definition at line 318 of file rootd.py.

13.4.3.11 tuple rootd.rootd_bpki_cert = rpki.x509.X509(Auto_file = cfg.get("rootd-bpki-cert"))

Definition at line 290 of file rootd.py.

13.4.3.12 tuple rootd.rootd_bpki_crl = rpki.x509.CRL(Auto_file = cfg.get("rootd-bpki-crl"))

Definition at line 291 of file rootd.py.

13.4.3.13 tuple rootd.rootd_bpki_key = rpki.x509.RSA(Auto_file = cfg.get("rootd-bpki-key"))

Definition at line 289 of file rootd.py.

13.4.3.14 tuple rootd.rpki_base_uri = cfg.get("rpki-base-uri", "rsync://" + rpki_class_name + ".invalid/")

Definition at line 300 of file rootd.py.

13.4.3.15 tuple rootd.rpki_class_name = cfg.get("rpki-class-name", "wombat")

Definition at line 297 of file rootd.py.

13.4.3.16 rootd.rpki_root_cert = None

Definition at line 46 of file rootd.py.

13.4.3.17 tuple rootd.rpki_root_cert_file = cfg.get("rpki-root-cert")

Definition at line 303 of file rootd.py.

13.4.3.18 tuple rootd.rpki_root_cert_uri = cfg.get("rpki-root-cert-uri", rpki_base_uri + "Root.cer")

Definition at line 304 of file rootd.py.

13.4.3.19 tuple rootd.rpki_root_crl = cfg.get("rpki-root-crl", "Root.crl")

Definition at line 307 of file rootd.py.

13.4.3.20 tuple rootd.rpki_root_dir = cfg.get("rpki-root-dir")

Definition at line 299 of file rootd.py.

13.4.3.21 tuple rootd.rpki_root_key = rpki.x509.RSA(Auto_file = cfg.get("rpki-root-key"))

Definition at line 302 of file rootd.py.

13.4.3.22 tuple rootd.rpki_root_manifest = cfg.get("rpki-root-manifest", "Root.mnf")

Definition at line 306 of file rootd.py.

13.4.3.23 tuple rootd.rpki_subject_cert = cfg.get("rpki-subject-cert", "Child.cer")

Definition at line 308 of file rootd.py.

13.4.3.24 tuple rootd.rpki_subject_lifetime = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-lifetime", "30d"))

Definition at line 311 of file rootd.py.

13.4.3.25 tuple rootd.rpki_subject_pkcs10 = cfg.get("rpki-subject-pkcs10", "Child.pkcs10")

Definition at line 309 of file rootd.py.

13.4.3.26 tuple rootd.rpki_subject_regen = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-regen", rpki_subject_lifetime.convert_to_seconds() / 2))

Definition at line 312 of file rootd.py.

13.4.3.27 rootd.server_cert = rootd_bpki_cert,

Definition at line 315 of file rootd.py.

13.5 Package rpki

Packages

- package __doc__
- package async
- package cli
- package config
- package exceptions
- package https
- package ipaddrs
- package left_right
- package log
- package manifest
- package myrpki
- package oids
- package publication
- package relaxng
- package resource_set
- package roa
- package rpki_engine
- package sql
- package sundial
- package up_down
- package x509
- package xml_utils

13.6 Package rpki.__doc__

13.7 Package rpki.async

Classes

- class gc_summary
- class iterator
- class sync_wrapper
- class timer

Functions

- def _raiseExitNow
- def defer
- def event_loop
- def exit_event_loop
- def run_deferred

Variables

- list deferred_queue = [ ]

  List to hold deferred actions.

- ExitNow = asyncore.ExitNow

13.7.1 Detailed Description

```
Utilities for event-driven programming.

$Id: async.py 3191 2010-04-12 23:07:16Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

13.7.2 Function Documentation

13.7.2.1 def rpki.async._raiseExitNow (*signum*, *frame*) [private]

```
Signal handler for event_loop().
```

Definition at line 269 of file async.py.

13.7.2.2 def rpki.async.defer (*thunk*)

```
Defer an action until the next pass through the event loop.
```

Definition at line 250 of file async.py.

13.7.2.3 def rpki.async.event_loop (*catch_signals* = (signal.SIGINT, signal.SIGTERM))

```
Replacement for asyncore.loop(), adding timer and signal support.
```

Definition at line 273 of file async.py.

13.7.2.4 def rpki.async.exit_event_loop ()

```
Force exit from event_loop().
```

Definition at line 364 of file async.py.

13.7.2.5 def rpki.async.run_deferred ()

```
Run deferred actions.
```

Definition at line 256 of file async.py.

13.7.3 Variable Documentation

13.7.3.1 rpki::async::deferred_queue = [ ]

List to hold deferred actions.

We used to do this with the timer queue, but that appears to confuse the garbage collector, and is overengineering for simple deferred actions in any case.

Definition at line 248 of file async.py.

13.7.3.2 rpki::async.ExitNow = asyncore.ExitNow

Definition at line 24 of file async.py.

13.8 Package rpki.cli

Classes

- class Cmd

Functions

- def yes_or_no

Variables

- dictionary _yes_or_no_prompts
- have_readline = True

13.8.1 Detailed Description

```
Utilities for writing command line tools.

$Id: cli.py 3191 2010-04-12 23:07:16Z sra $

Copyright (C) 2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

13.8.2 Function Documentation

13.8.2.1 def rpki.cli.yes_or_no (*prompt*, *default* = `None`, *require_full_word* = `False`)

```
Ask a yes-or-no question.
```

Definition at line 157 of file cli.py.

13.8.3 Variable Documentation

13.8.3.1 dictionary rpki::cli._yes_or_no_prompts

Initial value:

```
{
  True  : ' ("yes" or "no" ["yes"]) ',
  False : ' ("yes" or "no" ["no"]) ',
  None  : ' ("yes" or "no") ' }
```

Definition at line 172 of file cli.py.

13.8.3.2 rpki::cli.have_readline = True

Definition at line 25 of file cli.py.

13.9 Package rpki.config

Classes

- class parser

13.9.1 Detailed Description

```
Configuration file parsing utilities, layered on top of stock Python
ConfigParser module.

$Id: config.py 3107 2010-03-16 23:13:08Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
```

PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

13.10 Package rpki.exceptions

Classes

- class BadClassNameSyntax
- class BadClientURL
- class BadContactURL
- class BadExtension
- class BadIRDBReply
- class BadIssueResponse
- class BadPKCS10
- class BadPublicationReply
- class BadQuery
- class BadSender
- class BadStatusCode
- class BadURISyntax
- class BSCNotFound
- class BSCNotReady
- class ChildNotFound
- class ClassNameMismatch
- class ClassNameUnknown
- class ClientNotFound
- class CMSContentNotSet
- class CMSCRLNotSet
- class CMSVerificationFailed
- class DBConsistancyError
- class DERObjectConversionError
- class DuplicateObject
- class EmptyPEM
- class EmptyROAPrefixList

- class ForbiddenURI
- class HandleTranslationError
- class HTTPRequestFailed
- class HTTPSBadVersion
- class HTTPSClientAborted
- class HTTPSUnexpectedState
- class MissingCMSCRL
- class MissingCMSEEcert
- class MultipleTLSEECert
- class MustBePrefix
- class NoActiveCA
- class NoCoveringCertForROA
- class NoObjectAtURI
- class NotACertificateChain
- class NotFound
- class NotImplementedYet
- class NotInDatabase
- class ReceivedTLSCACert
- class RPKI_Exception
- class ServerShuttingDown
- class SKIMismatch
- class SubprocessError
- class TLSValidationError
- class UnexpectedCMSCerts
- class UnexpectedCMSCRLs
- class UnparsableCMSDER
- class UpstreamError
- class WrongEContentType

13.10.1 Detailed Description

```
Exception definitions for RPKI modules.

$Id: exceptions.py 2907 2009-12-23 20:48:19Z sra $

Copyright (C) 2009  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
```

OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

13.11 Package rpki.https

Classes

- class caller
- class http_client
- class http_listener
- class http_message
- class http_queue
- class http_request
- class http_response
- class http_server
- class http_stream

Functions

- def build_https_ta_cache
- def client
- def log_method
- def server

Variables

- dictionary client_queues = { }

  Map of (host, port) tuples to http_queue objects.

- debug_http = False

  Verbose chatter about HTTP streams.

- debug_tls_certs = False

  Verbose chatter about TLS certificates.

- tuple default_client_timeout = rpki.sundial.timedelta(minutes = 15)

  Default HTTP client connection timeout.

- tuple default_http_version = (1, 0)

  Preferred HTTP version.

- tuple default_server_timeout = rpki.sundial.timedelta(minutes = 20)

  Default HTTP server connection timeouts.

- string rpki_content_type = "application/x-rpki"

  HTTP content type used for all RPKI messages.

- tuple supported_address_families = (socket.AF_INET, socket.AF_INET6)

  IP address families to support.

- want_persistent_client = False

  Whether we want persistent HTTP client streams, when server also supports them.

- want_persistent_server = False

  Whether we want persistent HTTP server streams, when client also supports them.

13.11.1 Detailed Description

```
HTTPS utilities, both client and server.

$Id: https.py 3191 2010-04-12 23:07:16Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
```

```
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

13.11.2 Function Documentation

13.11.2.1 def rpki.https.build_https_ta_cache (*certs*)

```
Package up a collection of certificates into a form suitable for use
as a dynamic HTTPS trust anchor set.  Precise format of this
collection is an internal conspiracy within the rpki.https module;
at one point it was a POW.X509Store object, at the moment it's a
Python set, what it will be tomorow is nobody else's business.
```

Definition at line 1094 of file https.py.

13.11.2.2 def rpki.https.client (*msg*, *client_key*, *client_cert*, *server_ta*, *url*, *callback*, *errback*)

```
Open client HTTPS connection, send a message, set up callbacks to
handle response.
```

Definition at line 1034 of file https.py.

13.11.2.3 def rpki.https.log_method (*self*, *msg*, *logger* = rpki.log.debug)

```
Logging method used in several different classes.
```

Definition at line 235 of file https.py.

13.11.2.4 def rpki.https.server (*handlers*, *server_key*, *server_cert*, *port*, *host* = `""`, *client_ta* = `()`, *dynamic_https_trust_anchor* = `None`, *address_families* = `supported_address_families`)

```
Run an HTTPS server and wait (forever) for connections.
```

Definition at line 1079 of file https.py.

13.11.3 Variable Documentation

13.11.3.1 rpki::https::client_queues = {}

Map of (host, port) tuples to http_queue objects.

Definition at line 1032 of file https.py.

13.11.3.2 rpki::https::debug_http = False

Verbose chatter about HTTP streams.

Definition at line 45 of file https.py.

13.11.3.3 rpki::https::debug_tls_certs = False

Verbose chatter about TLS certificates.

Definition at line 49 of file https.py.

13.11.3.4 rpki::https::default_client_timeout = rpki.sundial.timedelta(minutes = 15)

Default HTTP client connection timeout.

Definition at line 61 of file https.py.

13.11.3.5 rpki::https::default_http_version = (1, 0)

Preferred HTTP version.

Definition at line 72 of file https.py.

13.11.3.6 rpki::https::default_server_timeout = rpki.sundial.timedelta(minutes = 20)

Default HTTP server connection timeouts.

Given our druthers, we'd prefer that the client close the connection, as this avoids the problem of client starting to reuse connection just as server closes it, so this should be longer than the client timeout.

Definition at line 68 of file https.py.

13.11.3.7 rpki::https::rpki_content_type = "application/x-rpki"

HTTP content type used for all RPKI messages.

Definition at line 41 of file https.py.

13.11.3.8 tuple rpki::https::supported_address_families = (socket.AF_INET, socket.AF_INET6)

IP address families to support.

Almost all the code is in place for IPv6, the missing bits are DNS support that would let us figure out which address family to request, and configuration support to let us figure out which protocols are supported on the local machine. For now, leave code in place but disabled.

Address families on which to listen; first entry is also the default for opening new connections.

Definition at line 85 of file https.py.

13.11.3.9 rpki::https::want_persistent_client = False

Whether we want persistent HTTP client streams, when server also supports them.

Definition at line 53 of file https.py.

13.11.3.10 rpki::https::want_persistent_server = False

Whether we want persistent HTTP server streams, when client also supports them.

Definition at line 57 of file https.py.

13.12 Package rpki.ipaddrs

Classes

- class v4addr
- class v6addr

13.12.1 Detailed Description

```
Classes to represent IP addresses.

Given some of the other operations we need to perform on them, it's
most convenient to represent IP addresses as Python "long" values.
The classes in this module just wrap suitable read/write syntax around
the underlying "long" type.

These classes also supply a "bits" attribute for use by other code
built on these classes; for the most part, IPv6 addresses really are
just IPv4 addresses with more bits, so we supply the number of bits
once, here, thus avoiding a lot of duplicate code elsewhere.

$Id: ipaddrs.py 2424 2009-05-11 06:37:32Z sra $

Copyright (C) 2009  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
```

```
PERFORMANCE OF THIS SOFTWARE.
```

13.13 Package rpki.left_right

Classes

- class bsc_elt
- class child_elt
- class cms_msg
- class data_elt
- class left_right_namespace
- class list_published_objects_elt
- class list_received_resources_elt
- class list_resources_elt
- class list_roa_requests_elt
- class msg
- class parent_elt
- class report_error_elt
- class repository_elt
- class sax_handler
- class self_elt

Variables

- enforce_strict_up_down_xml_sender = False

13.13.1 Detailed Description

```
RPKI "left-right" protocol.

$Id: left_right.py 3191 2010-04-12 23:07:16Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

Portions copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

13.13.2 Variable Documentation

13.13.2.1 rpki::left_right.enforce_strict_up_down_xml_sender = False

Definition at line 40 of file left_right.py.

13.14 Package rpki.log

Classes

- class logger

Functions

- def init
- def set_trace
- def trace
- def traceback

Variables

- tuple debug = logger(syslog.LOG_DEBUG)
- enable_trace = False

  Whether call tracing is enabled.

- tuple error = logger(syslog.LOG_ERR)
- tuple info = logger(syslog.LOG_INFO)
- tuple note = logger(syslog.LOG_NOTICE)
- int pid = 0

- string tag = ""
- use_syslog = True

  Whether to use syslog.

- tuple warn = logger(syslog.LOG_WARNING)

13.14.1 Detailed Description

```
Logging facilities for RPKI libraries.

$Id: log.py 3107 2010-03-16 23:13:08Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

13.14.2 Function Documentation

13.14.2.1 def rpki.log.init (*ident* = `"rpki"`, *flags* = `syslog.LOG_PID`, *facility* = `syslog.LOG_DAEMON`)

```
Initialize logging system.
```

Definition at line 51 of file log.py.

13.14.2.2 def rpki.log.set_trace (*enable*)

```
Enable or disable call tracing.
```

Definition at line 63 of file log.py.

13.14.2.3 def rpki.log.trace ()

```
Execution trace -- where are we now, and whence came we here?
```

Definition at line 91 of file log.py.

13.14.2.4 def rpki.log.traceback ()

```
Consolidated backtrace facility with a bit of extra info.
```

Definition at line 100 of file log.py.

13.14.3 Variable Documentation

13.14.3.1 tuple rpki::log.debug = logger(syslog.LOG_DEBUG)

Definition at line 89 of file log.py.

13.14.3.2 rpki::log::enable_trace = False

Whether call tracing is enabled.

Definition at line 41 of file log.py.

13.14.3.3 tuple rpki::log.error = logger(syslog.LOG_ERR)

Definition at line 85 of file log.py.

13.14.3.4 tuple rpki::log.info = logger(syslog.LOG_INFO)

Definition at line 88 of file log.py.

13.14.3.5 tuple rpki::log.note = logger(syslog.LOG_NOTICE)

Definition at line 87 of file log.py.

13.14.3.6 int rpki::log.pid = 0

Definition at line 49 of file log.py.

13.14.3.7 string rpki::log.tag = ""

Definition at line 48 of file log.py.

13.14.3.8 rpki::log::use_syslog = True

Whether to use syslog.

Definition at line 46 of file log.py.

13.14.3.9 tuple rpki::log.warn = logger(syslog.LOG_WARNING)

Definition at line 86 of file log.py.

13.15 Package rpki.manifest

Classes

- class FileAndHash
- class FilesAndHashes
- class Manifest

13.15.1 Detailed Description

```
Signed manifests.  This is just the ASN.1 encoder, the rest is in
rpki.x509 with the rest of the DER_object code.

Note that rpki.x509.SignedManifest implements the signed manifest;
the structures here are just the payload of the CMS eContent field.

$Id: manifest.py 2424 2009-05-11 06:37:32Z sra $
```


```
Copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```


13.16 Package rpki.myrpki

Classes

- class CA
- class child
- class children
- class comma_set
- class csv_reader
- class EntityDB
- class main
- class parent
- class parents
- class repositories
- class repository
- class roa_request
- class roa_requests

Functions

- def b64_equal
- def csv_writer
- def etree_post_read
- def etree_pre_write

- def etree_read
- def etree_validate
- def etree_write
- def PEMElement

Variables

- allow_incomplete = False
- string namespace = "http://www.hactrn.net/uris/rpki/myrpki/"
- string namespaceQName = "{"
- string version = "2"
- whine = False

13.16.1 Detailed Description

```
This (oversized) module used to be an (oversized) program.
Refactoring in progress, some doc still needs updating.


This program is now the merger of three different tools: the old
myrpki.py script, the old myirbe.py script, and the newer setup.py CLI
tool.  As such, it is still in need of some cleanup, but the need to
provide a saner user interface is more urgent than internal code
prettiness at the moment.  In the long run, 90% of the code in this
file probably ought to move to well-designed library modules.

Overall goal here is to build up the configuration necessary to run
rpkid and friends, by reading a config file, a collection of .CSV
files, and the results of a few out-of-band XML setup messages
exchanged with one's parents, children, and so forth.

The config file is in an OpenSSL-compatible format, the CSV files are
simple tab-delimited text.  The XML files are all generated by this
program, either the local instance or an instance being run by another
player in the system; the mechanism used to exchange these setup
messages is outside the scope of this program, feel free to use
PGP-signed mail, a web interface (not provided), USB stick, carrier
pigeons, whatever works.

With one exception, the commands in this program avoid using any
third-party Python code other than the rpki libraries themselves; with
the same one exception, all OpenSSL work is done with the OpenSSL
command line tool (the one built as a side effect of building rcynic
will do, if your platform has no system copy or the system copy is too
old).  This is all done in an attempt to make the code more portable,
so one can run most of the RPKI back end software on a laptop or
whatever.  The one exception is the configure_daemons command, which
must, of necessity, use the same communication libraries as the
daemons with which it is conversing.  So that one command will not
work if the correct Python modules are not available.
```

```
$Id: myrpki.py -1   $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

13.16.2 Function Documentation

13.16.2.1 def rpki.myrpki.b64_equal (*thing1*, *thing2*)

```
Compare two Base64-encoded values for equality.
```

Definition at line 843 of file myrpki.py.

13.16.2.2 def rpki.myrpki.csv_writer (*filename*)

```
Writer object for tab delimited text.  We just use the stock CSV
module in excel-tab mode for this.
```

Definition at line 520 of file myrpki.py.

13.16.2.3 def rpki.myrpki.etree_post_read (*e*, *validate* = **True**)

```
Do the namespace frobbing needed on read; broken out of etree_read()
beause also needed by ElementFromString().
```

Definition at line 829 of file myrpki.py.

13.16.2.4 def rpki.myrpki.etree_pre_write (*e*, *validate* = **True**)

```
Do the namespace frobbing needed on write; broken out of
etree_write() because also needed with ElementToString().
```

Definition at line 804 of file myrpki.py.

13.16.2.5 def rpki.myrpki.etree_read (*filename*, *verbose* = `False`, *validate* = `True`)

```
Read an etree from a file, verifying then stripping XML namespace
cruft.
```

Definition at line 819 of file myrpki.py.

13.16.2.6 def rpki.myrpki.etree_validate (*e*)

Definition at line 768 of file myrpki.py.

13.16.2.7 def rpki.myrpki.etree_write (*e*, *filename*, *verbose* = `False`, *validate* = `True`, *msg* = `None`)

```
Write out an etree to a file, safely.

I still miss SYSCAL(RENMWO).
```

Definition at line 785 of file myrpki.py.

13.16.2.8 def rpki.myrpki.PEMElement (*e*, *tag*, *filename*, *kwargs*)

```
Create an XML element containing Base64 encoded data taken from a
PEM file.
```

Definition at line 528 of file myrpki.py.

13.16.3 Variable Documentation

13.16.3.1 rpki::myrpki.allow_incomplete = False

Definition at line 80 of file myrpki.py.

13.16.3.2 string rpki::myrpki.namespace = "http://www.hactrn.net/uris/rpki/myrpki/"

Definition at line 74 of file myrpki.py.

13.16.3.3 string rpki::myrpki.namespaceQName = "{"

Definition at line 76 of file myrpki.py.

13.16.3.4 string rpki::myrpki.version = "2"

Definition at line 75 of file myrpki.py.

13.16.3.5 rpki::myrpki.whine = False

Definition at line 84 of file myrpki.py.

13.17 Package rpki.oids

Variables

- tuple name2oid = dict((v, k) for k, v in oid2name.items())

  Mapping table of string names to OIDs.

- dictionary oid2name

  Mapping table of OIDs to conventional string names.

13.17.1 Detailed Description

```
OID database.

$Id: oids.py 2424 2009-05-11 06:37:32Z sra $
```

Copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

13.17.2 Variable Documentation

13.17.2.1 rpki::oids::name2oid = dict((v, k) for k, v in oid2name.items())

Mapping table of string names to OIDs.

Definition at line 58 of file oids.py.

13.17.2.2 rpki::oids::oid2name

Initial value:

```
{
  (1, 2, 840, 113549, 1, 1, 11)         : "sha256WithRSAEncryption",
  (1, 2, 840, 113549, 1, 1, 12)         : "sha384WithRSAEncryption",
  (1, 2, 840, 113549, 1, 1, 13)         : "sha512WithRSAEncryption",
  (1, 2, 840, 113549, 1, 7,  1)         : "id-data",
  (1, 2, 840, 113549, 1, 9, 16)         : "id-smime",
  (1, 2, 840, 113549, 1, 9, 16, 1)      : "id-ct",
  (1, 2, 840, 113549, 1, 9, 16, 1, 24)  : "id-ct-routeOriginAttestation",
  (1, 2, 840, 113549, 1, 9, 16, 1, 26)  : "id-ct-rpkiManifest",
  (1, 2, 840, 113549, 1, 9, 16, 1, 28)  : "id-ct-xml",
  (1, 3, 6, 1, 5, 5, 7, 1, 1)           : "authorityInfoAccess",
  (1, 3, 6, 1, 5, 5, 7, 1, 11)          : "subjectInfoAccess",
  (1, 3, 6, 1, 5, 5, 7, 1, 7)           : "sbgp-ipAddrBlock",
  (1, 3, 6, 1, 5, 5, 7, 1, 8)           : "sbgp-autonomousSysNum",
  (1, 3, 6, 1, 5, 5, 7, 14, 2)          : "id-cp-ipAddr-asNumber",
  (1, 3, 6, 1, 5, 5, 7, 48, 2)          : "id-ad-caIssuers",
  (1, 3, 6, 1, 5, 5, 7, 48, 5)          : "id-ad-caRepository",
  (1, 3, 6, 1, 5, 5, 7, 48, 9)          : "id-ad-signedObjectRepository",
  (1, 3, 6, 1, 5, 5, 7, 48, 10)         : "id-ad-rpkiManifest",
  (1, 3, 6, 1, 5, 5, 7, 48, 11)         : "id-ad-signedObject",
  (2, 16, 840, 1, 101, 3, 4, 2, 1)      : "id-sha256",
  (2, 5, 29, 14)                        : "subjectKeyIdentifier",
  (2, 5, 29, 15)                        : "keyUsage",
  (2, 5, 29, 19)                        : "basicConstraints",
  (2, 5, 29, 20)                        : "cRLNumber",
```

```
  (2, 5, 29, 31)                        : "cRLDistributionPoints",
  (2, 5, 29, 32)                        : "certificatePolicies",
  (2, 5, 29, 35)                        : "authorityKeyIdentifier",
  (2, 5, 4, 3)                          : "commonName",
}
```

Mapping table of OIDs to conventional string names.

Definition at line 24 of file oids.py.

13.18 Package rpki.publication

Classes

- class certificate_elt
- class client_elt
- class cms_msg
- class config_elt
- class control_elt
- class crl_elt
- class manifest_elt
- class msg
- class publication_namespace
- class publication_object_elt
- class report_error_elt
- class roa_elt
- class sax_handler

13.18.1 Detailed Description

```
RPKI "publication" protocol.

$Id: publication.py 3107 2010-03-16 23:13:08Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

Portions copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

13.19 Package rpki.relaxng

Variables

- tuple left_right

  Parsed RelaxNG left_right schema.

- tuple publication

  Parsed RelaxNG publication schema.

- tuple up_down

  Parsed RelaxNG up_down schema.

13.19.1 Variable Documentation

13.19.1.1 rpki::relaxng::left_right

Parsed RelaxNG left_right schema.

Definition at line 7 of file relaxng.py.

13.19.1.2 rpki::relaxng::publication

Parsed RelaxNG publication schema.

Definition at line 1252 of file relaxng.py.

13.19.1.3 rpki::relaxng::up_down

Parsed RelaxNG up_down schema.

Definition at line 998 of file relaxng.py.

13.20 Package rpki.resource_set

Classes

- class resource_bag
- class resource_range
- class resource_range_as
- class resource_range_ip
- class resource_range_ipv4
- class resource_range_ipv6
- class resource_set
- class resource_set_as
- class resource_set_ip
- class resource_set_ipv4
- class resource_set_ipv6
- class roa_prefix
- class roa_prefix_ipv4
- class roa_prefix_ipv6
- class roa_prefix_set
- class roa_prefix_set_ipv4
- class roa_prefix_set_ipv6

Functions

- def _bs2long
- def _long2bs
- def _rsplit
- def test1
- def test2

Variables

- string inherit_token = "<inherit>"

  Token used to indicate inheritance in read and print syntax.

13.20.1 Detailed Description

```
Classes dealing with sets of resources.

The basic mechanics of a resource set are the same for any of the
resources we handle (ASNs, IPv4 addresses, or IPv6 addresses), so we
can provide the same operations on any of them, even though the
underlying details vary.

We also provide some basic set operations (union, intersection, etc).

$Id: resource_set.py 3107 2010-03-16 23:13:08Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

13.20.2 Function Documentation

13.20.2.1 def rpki.resource_set._bs2long (*bs*, *addrlen*, *fill*) [private]

```
Utility function to convert a bitstring (POW.pkix tuple
representation) into a Python long.
```

Definition at line 514 of file resource_set.py.

13.20.2.2 def rpki.resource_set._long2bs (*number*, *addrlen*, *prefixlen* = `None`, *strip* = `None`) `[private]`

```
Utility function to convert a Python long into a POW.pkix tuple
bitstring.  This is a bit complicated because it supports the
fiendishly compact encoding used in RFC 3779.
```

Definition at line 526 of file resource_set.py.

13.20.2.3 def rpki.resource_set._rsplit (*rset*, *that*) `[private]`

```
Utility function to split a resource range into two resource ranges.
```

Definition at line 190 of file resource_set.py.

13.20.2.4 def rpki.resource_set.test1 (*t*, *s1*, *s2*)

Definition at line 884 of file resource_set.py.

13.20.2.5 def rpki.resource_set.test2 (*t*, *s1*, *s2*)

Definition at line 917 of file resource_set.py.

13.20.3 Variable Documentation

13.20.3.1 rpki::resource_set::inherit_token = "<inherit>"

Token used to indicate inheritance in read and print syntax.

Definition at line 48 of file resource_set.py.

13.21 Package rpki.roa

Classes

- class ROAIPAddress

- class ROAIPAddresses
- class ROAIPAddressFamilies
- class ROAIPAddressFamily
- class RouteOriginAttestation

13.21.1 Detailed Description

```
ROA (Route Origin Authorization).

At the moment this is just the ASN.1 encoder.

This corresponds to draft-ietf-sidr-roa-format, which is a work in
progress, so this may need updating later.

$Id: roa.py 2424 2009-05-11 06:37:32Z sra $

Copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

draft-ietf-sidr-roa-format-03 2.1.3.2 specifies:

   RouteOriginAttestation ::= SEQUENCE {
      version [0] INTEGER DEFAULT 0,
      asID  ASID,
      ipAddrBlocks SEQUENCE OF ROAIPAddressFamily }

   ASID ::= INTEGER

   ROAIPAddressFamily ::= SEQUENCE {
      addressFamily OCTET STRING (SIZE (2..3)),
      addresses SEQUENCE OF ROAIPAddress }

   ROAIPAddress ::= SEQUENCE {
      address IPAddress,
      maxLength INTEGER OPTIONAL }

   IPAddress ::= BIT STRING
```

13.22 Package rpki.rpki_engine

Classes

- class ca_detail_obj
- class ca_obj
- class child_cert_obj
- class publication_queue
- class revoked_cert_obj
- class roa_obj
- class rpkid_context

13.22.1 Detailed Description

```
Global context for rpkid.

$Id: rpki_engine.py 3107 2010-03-16 23:13:08Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

13.23 Package rpki.sql

Classes

- class session

- class sql_persistent
- class template

13.23.1 Detailed Description

```
SQL interface code.

$Id: sql.py 2895 2009-12-21 17:17:55Z sra $

Copyright (C) 2009  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

13.24 Package rpki.sundial

Classes

- class datetime
- class timedelta

Functions

- def _cast
- def now
- def test

13.24.1 Detailed Description

```
Unified RPKI date/time handling, based on the standard Python datetime module.

Module name chosen to sidestep a nightmare of import-related errors
that occur with the more obvious module names.

List of arithmetic methods that require result casting was derived by
inspection of the datetime module, to wit:

  >>> import datetime
  >>> for t in (datetime.datetime, datetime.timedelta):
  ...  for k in t.__dict__.keys():
  ...   if k.startswith("__"):
  ...    print "%s.%s()" % (t.__name__, k)

$Id: sundial.py 3191 2010-04-12 23:07:16Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

13.24.2 Function Documentation

13.24.2.1 def rpki.sundial._cast (*x*) [private]

```
Cast result of arithmetic operations back into correct subtype.
```

Definition at line 257 of file sundial.py.

13.24.2.2 def rpki.sundial.now ()

```
Get current timestamp.
```

Definition at line 50 of file sundial.py.

13.24.2.3 def rpki.sundial.test (*t*)

Definition at line 269 of file sundial.py.

13.25 Package rpki.up_down

Classes

- class base_elt
- class certificate_elt
- class class_elt
- class class_response_syntax
- class cms_msg
- class error_response_pdu
- class issue_pdu
- class issue_response_pdu
- class list_pdu
- class list_response_pdu
- class message_pdu
- class multi_uri
- class revoke_pdu
- class revoke_response_pdu
- class revoke_syntax
- class sax_handler

Variables

- dictionary nsmap = { None : xmlns }
- string xmlns = "http://www.apnic.net/specs/rescerts/up-down/"

13.25.1 Detailed Description

```
RPKI "up-down" protocol.

$Id: up_down.py 3162 2010-04-06 18:50:47Z sra $

Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

13.25.2 Variable Documentation

13.25.2.1 dictionary rpki::up_down.nsmap = { None : xmlns }

Definition at line 41 of file up_down.py.

13.25.2.2 string rpki::up_down.xmlns = "http://www.apnic.net/specs/rescerts/up-down/"

Definition at line 39 of file up_down.py.

13.26 Package rpki.x509

Classes

- class CMS_object
- class CRL
- class DeadDrop
- class DER_CMS_object
- class DER_object
- class PEM_converter
- class PKCS10
- class ROA
- class RSA
- class RSApublic
- class SignedManifest
- class X509
- class XML_CMS_object

Functions

- def _find_xia_uri
- def calculate_SKI
- def POWify_OID

13.26.1 Detailed Description

```
One X.509 implementation to rule them all...

...and in the darkness hide the twisty maze of partially overlapping
X.509 support packages in Python.

There are several existing packages, none of which do quite what I
need, due to age, lack of documentation, specialization, or lack of
foresight on somebody's part (perhaps mine).  This module attempts to
bring together the functionality I need in a way that hides at least
some of the nasty details.  This involves a lot of format conversion.

$Id: x509.py 3107 2010-03-16 23:13:08Z sra $


Copyright (C) 2009-2010  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
```

AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

13.26.2 Function Documentation

13.26.2.1 def rpki.x509._find_xia_uri (*extension*, *name*) [private]

```
Find a rsync URI in an SIA or AIA extension.
Returns the URI if found, otherwise None.
```

Definition at line 105 of file x509.py.

13.26.2.2 def rpki.x509.calculate_SKI (*public_key_der*)

```
Calculate the SKI value given the DER representation of a public
key, which requires first peeling the ASN.1 wrapper off the key.
```

Definition at line 51 of file x509.py.

13.26.2.3 def rpki.x509.POWify_OID (*oid*)

```
Utility function to convert tuple form of an OID to the
dotted-decimal string form that POW uses.
```

Definition at line 725 of file x509.py.

13.27 Package rpki.xml_utils

Classes

- class base_elt
- class data_elt
- class msg
- class sax_handler
- class text_elt

13.27.1 Detailed Description

```
XML utilities.

$Id: xml_utils.py 2836 2009-10-26 22:31:16Z sra $

Copyright (C) 2009  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

13.28 Package rpkid

Functions

- def main

Variables

- string cfg_file = "rpkid.conf"
- profile = None

13.28.1 Detailed Description

```
RPKI engine daemon.  This is still very much a work in progress.

Usage: python rpkid.py [ { -c | --config } configfile ]
                   [ { -h | --help } ]
                   [ { -p | --profile } outputfile ]

Default configuration file is rpkid.conf, override with --config option.

$Id: rpkid.py 2913 2009-12-28 20:55:38Z sra $

Copyright (C) 2009  Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008  American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any
purpose with or without fee is hereby granted, provided that the above
copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH
REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY
AND FITNESS.  IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT,
INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM
LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE
OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
PERFORMANCE OF THIS SOFTWARE.
```

13.28.2 Function Documentation

13.28.2.1 def rpkid.main ()

Definition at line 68 of file rpkid.py.

13.28.3 Variable Documentation

13.28.3.1 rpkid.cfg_file = "rpkid.conf"

Definition at line 49 of file rpkid.py.

13.28.3.2 rpkid.profile = None

Definition at line 50 of file rpkid.py.

14 Class Documentation

14.1 async_chat Class Reference

Inherited by rpki.https.http_stream.

The documentation for this class was generated from the following file:

- https.py (3191)

14.2 dispatcher Class Reference

Inherited by rpki.https.http_listener.

The documentation for this class was generated from the following file:

- https.py (3191)

14.3 Cmd Class Reference

Inherited by rpki.cli.Cmd.

The documentation for this class was generated from the following file:

- cli.py (3191)

14.4 dict Class Reference

Inherited by rpki.myrpki.children, rpki.myrpki.parents, rpki.myrpki.repositories, and rpki.myrpki.roa_requests.

The documentation for this class was generated from the following file:

- myrpki.py

14.5 Exception Class Reference

Inherited by rpki.exceptions.RPKI_Exception.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.6 irbe_cli.bsc_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::bsc_elt.

Collaboration diagram for irbe_cli.bsc_elt:

Public Member Functions

- def client_query_signing_cert
- def client_query_signing_cert_crl
- def client_reply_decode

Public Attributes

- signing_cert
- signing_cert_crl

Static Public Attributes

- tuple excludes = ("pkcs10_request",)

  XML attributes and elements that should not be allowed as command line arguments.

14.6.1 Detailed Description

Definition at line 152 of file irbe_cli.py.

14.6.2 Member Function Documentation

14.6.2.1 def irbe_cli.bsc_elt.client_query_signing_cert (*self*, *arg*)

```
--signing_cert option.
```

Definition at line 156 of file irbe_cli.py.

14.6.2.2 def irbe_cli.bsc_elt.client_query_signing_cert_crl (*self*, *arg*)

```
--signing_cert_crl option.
```

Definition at line 160 of file irbe_cli.py.

14.6.2.3 def irbe_cli.bsc_elt.client_reply_decode (*self*)

Reimplemented from irbe_cli.reply_elt_mixin.

Definition at line 164 of file irbe_cli.py.

14.6.3 Member Data Documentation

14.6.3.1 tuple irbe_cli.bsc_elt.excludes = ("pkcs10_request",) `[static]`

XML attributes and elements that should not be allowed as command line arguments.

Reimplemented from irbe_cli.cmd_elt_mixin.

Definition at line 154 of file irbe_cli.py.

14.6.3.2 irbe_cli.bsc_elt.signing_cert

Reimplemented from rpki.left_right.bsc_elt.

Definition at line 158 of file irbe_cli.py.

14.6.3.3 irbe_cli.bsc_elt.signing_cert_crl

Reimplemented from rpki.left_right.bsc_elt.

Definition at line 162 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.7 irbe_cli.certificate_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::certificate_elt.

Collaboration diagram for irbe_cli.certificate_elt:

14.7.1 Detailed Description

Definition at line 211 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.8 irbe_cli.child_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::child_elt.

Collaboration diagram for irbe_cli.child_elt:

14.8.1 Detailed Description

Definition at line 174 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.9 irbe_cli.client_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::client_elt.

Collaboration diagram for irbe_cli.client_elt:

14.9.1 Detailed Description

Definition at line 208 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.10 irbe_cli.cmd_elt_mixin Class Reference

Inherits irbe_cli::reply_elt_mixin.

Inherited by irbe_cli.bsc_elt, irbe_cli.certificate_elt, irbe_cli.child_elt, irbe_cli.client_elt, irbe_cli.config_elt, irbe_cli.crl_elt, irbe_cli.list_published_objects_elt, irbe_cli.list_received_resources_elt, irbe_cli.manifest_elt, irbe_cli.parent_elt, irbe_cli.repository_elt, irbe_cli.roa_elt, and irbe_cli.self_elt.

Collaboration diagram for irbe_cli.cmd_elt_mixin:

Public Member Functions

- def client_getopt
- def client_query_bpki_cert
- def client_query_bpki_cms_cert
- def client_query_bpki_https_cert
- def client_query_cms_glue

- def client_query_glue
- def client_query_https_glue
- def usage

Public Attributes

- bpki_cert
- bpki_cms_cert
- bpki_cms_glue
- bpki_glue
- bpki_https_cert
- bpki_https_glue

Static Public Attributes

- tuple excludes = ()

  XML attributes and elements that should not be allowed as command line arguments.

- is_cmd = True

14.10.1 Detailed Description

```
Protocol mix-in for command line client element PDUs.
```

Definition at line 68 of file irbe_cli.py.

14.10.2 Member Function Documentation

14.10.2.1 def irbe_cli.cmd_elt_mixin.client_getopt (*self*, *argv*)

```
Parse options for this class.
```

Definition at line 92 of file irbe_cli.py.

14.10.2.2 def irbe_cli.cmd_elt_mixin.client_query_bpki_cert (*self*, *arg*)

```
Special handler for --bpki_cert option.
```

Definition at line 109 of file irbe_cli.py.

14.10.2.3 def irbe_cli.cmd_elt_mixin.client_query_bpki_cms_cert (*self*, *arg*)

```
Special handler for --bpki_cms_cert option.
```

Definition at line 117 of file irbe_cli.py.

14.10.2.4 def irbe_cli.cmd_elt_mixin.client_query_bpki_https_cert (*self*, *arg*)

```
Special handler for --bpki_https_cert option.
```

Definition at line 125 of file irbe_cli.py.

14.10.2.5 def irbe_cli.cmd_elt_mixin.client_query_cms_glue (*self*, *arg*)

```
Special handler for --bpki_cms_glue option.
```

Definition at line 121 of file irbe_cli.py.

14.10.2.6 def irbe_cli.cmd_elt_mixin.client_query_glue (*self*, *arg*)

```
Special handler for --bpki_glue option.
```

Definition at line 113 of file irbe_cli.py.

14.10.2.7 def irbe_cli.cmd_elt_mixin.client_query_https_glue (*self*, *arg*)

```
Special handler for --bpki_https_glue option.
```

Definition at line 129 of file irbe_cli.py.

14.10.2.8 def irbe_cli.cmd_elt_mixin.usage (*cls*)

```
Generate usage message for this PDU.
```

Definition at line 81 of file irbe_cli.py.

14.10.3 Member Data Documentation

14.10.3.1 irbe_cli.cmd_elt_mixin.bpki_cert

Definition at line 111 of file irbe_cli.py.

14.10.3.2 irbe_cli.cmd_elt_mixin.bpki_cms_cert

Definition at line 119 of file irbe_cli.py.

14.10.3.3 irbe_cli.cmd_elt_mixin.bpki_cms_glue

Definition at line 123 of file irbe_cli.py.

14.10.3.4 irbe_cli.cmd_elt_mixin.bpki_glue

Definition at line 115 of file irbe_cli.py.

14.10.3.5 irbe_cli.cmd_elt_mixin.bpki_https_cert

Definition at line 127 of file irbe_cli.py.

14.10.3.6 irbe_cli.cmd_elt_mixin.bpki_https_glue

Definition at line 131 of file irbe_cli.py.

14.10.3.7 irbe_cli.cmd_elt_mixin::excludes = () `[static]`

XML attributes and elements that should not be allowed as command line arguments.

Reimplemented in irbe_cli.bsc_elt, irbe_cli.list_published_objects_elt, and irbe_cli.list_received_resources_elt.

Definition at line 78 of file irbe_cli.py.

14.10.3.8 irbe_cli.cmd_elt_mixin.is_cmd = True [static]

Reimplemented from irbe_cli.reply_elt_mixin.

Definition at line 73 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.11 irbe_cli.cmd_msg_mixin Class Reference

Inherits object.

Inherited by irbe_cli.left_right_msg, and irbe_cli.publication_msg.

Collaboration diagram for irbe_cli.cmd_msg_mixin:

Public Member Functions

- def usage

14.11.1 Detailed Description

```
Protocol mix-in for command line client message PDUs.
```

Definition at line 133 of file irbe_cli.py.

14.11.2 Member Function Documentation

14.11.2.1 def irbe_cli.cmd_msg_mixin.usage (*cls*)

```
Generate usage message for this PDU.
```

Definition at line 139 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.12 irbe_cli.config_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::config_elt.

Collaboration diagram for irbe_cli.config_elt:

Public Member Functions

- def client_query_bpki_crl

Public Attributes

- bpki_crl

14.12.1 Detailed Description

Definition at line 202 of file irbe_cli.py.

14.12.2 Member Function Documentation

14.12.2.1 def irbe_cli.config_elt.client_query_bpki_crl (*self*, *arg*)

```
Special handler for --bpki_crl option.
```

Definition at line 204 of file irbe_cli.py.

14.12.3 Member Data Documentation

14.12.3.1 irbe_cli.config_elt.bpki_crl

Definition at line 206 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.13 irbe_cli.crl_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::crl_elt.

Collaboration diagram for irbe_cli.crl_elt:

14.13.1 Detailed Description

Definition at line 214 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.14 irbe_cli.left_right_cms_msg Class Reference

Inherits rpki::left_right::cms_msg.

Collaboration diagram for irbe_cli.left_right_cms_msg:

Static Public Attributes

- saxify = left_right_sax_handler.saxify

14.14.1 Detailed Description

Definition at line 197 of file irbe_cli.py.

14.14.2 Member Data Documentation

14.14.2.1 irbe_cli.left_right_cms_msg.saxify = left_right_sax_handler.saxify [static]

Reimplemented from rpki.left_right.cms_msg.

Definition at line 198 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.15 irbe_cli.left_right_msg Class Reference

Inherits irbe_cli::cmd_msg_mixin, and rpki::left_right::msg.

Collaboration diagram for irbe_cli.left_right_msg:

Static Public Attributes

- tuple pdus

  Dispatch table of PDUs for this protocol.

14.15.1 Detailed Description

Definition at line 189 of file irbe_cli.py.

14.15.2 Member Data Documentation

14.15.2.1 tuple irbe_cli.left_right_msg.pdus [static]

Initial value:

```
dict((x.element_name, x)
              for x in (self_elt, bsc_elt, parent_elt, child_elt, repository_elt,

                        list_published_objects_elt, list_received_resources_elt,
      report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented from rpki.left_right.msg.

Definition at line 190 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.16 irbe_cli.left_right_proto Class Reference

Inherits object.

Collaboration diagram for irbe_cli.left_right_proto:

Static Public Attributes

- cms_msg = left_right_cms_msg
- msg = left_right_msg

14.16.1 Detailed Description

Definition at line 302 of file irbe_cli.py.

14.16.2 Member Data Documentation

14.16.2.1 irbe_cli.left_right_proto.cms_msg = left_right_cms_msg [static]

Definition at line 303 of file irbe_cli.py.

14.16.2.2 irbe_cli.left_right_proto.msg = left_right_msg [static]

Definition at line 304 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.17 irbe_cli.left_right_sax_handler Class Reference

Inherits rpki::left_right::sax_handler.

Collaboration diagram for irbe_cli.left_right_sax_handler:

Static Public Attributes

- pdu = left_right_msg

14.17.1 Detailed Description

Definition at line 194 of file irbe_cli.py.

14.17.2 Member Data Documentation

14.17.2.1 irbe_cli.left_right_sax_handler.pdu = left_right_msg [static]

Reimplemented from rpki.left_right.sax_handler.

Definition at line 195 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.18 irbe_cli.list_published_objects_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::list_published_objects_elt.

Collaboration diagram for irbe_cli.list_published_objects_elt:

Static Public Attributes

- tuple excludes = ("uri",)

XML attributes and elements that should not be allowed as command line arguments.

14.18.1 Detailed Description

Definition at line 180 of file irbe_cli.py.

14.18.2 Member Data Documentation

14.18.2.1 tuple irbe_cli.list_published_objects_elt.excludes = ("uri",) [static]

XML attributes and elements that should not be allowed as command line arguments.

Reimplemented from irbe_cli.cmd_elt_mixin.

Definition at line 181 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.19 irbe_cli.list_received_resources_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::list_received_resources_elt.

Collaboration diagram for irbe_cli.list_received_resources_elt:

Static Public Attributes

- tuple excludes = ("notBefore", "notAfter", "uri", "sia_uri", "aia_uri", "asn", "ipv4", "ipv6")

  XML attributes and elements that should not be allowed as command line arguments.

14.19.1 Detailed Description

Definition at line 183 of file irbe_cli.py.

14.19.2 Member Data Documentation

14.19.2.1 tuple irbe_cli.list_received_resources_elt.excludes = ("notBefore", "notAfter", "uri", "sia_uri", "aia_uri", "asn", "ipv4", "ipv6") [static]

XML attributes and elements that should not be allowed as command line arguments.

Reimplemented from irbe_cli.cmd_elt_mixin.

Definition at line 184 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.20 irbe_cli.manifest_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::manifest_elt.

Collaboration diagram for irbe_cli.manifest_elt:

14.20.1 Detailed Description

Definition at line 217 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.21 irbe_cli.parent_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::parent_elt.

Collaboration diagram for irbe_cli.parent_elt:

14.21.1 Detailed Description

Definition at line 171 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.22 irbe_cli.publication_cms_msg Class Reference

Inherits rpki::publication::cms_msg.

Collaboration diagram for irbe_cli.publication_cms_msg:

Static Public Attributes

- saxify = publication_sax_handler.saxify

14.22.1 Detailed Description

Definition at line 233 of file irbe_cli.py.

14.22.2 Member Data Documentation

14.22.2.1 irbe_cli.publication_cms_msg.saxify = publication_sax_handler.saxify [static]

Reimplemented from rpki.publication.cms_msg.

Definition at line 234 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.23 irbe_cli.publication_msg Class Reference

Inherits irbe_cli::cmd_msg_mixin, and rpki::publication::msg.

Collaboration diagram for irbe_cli.publication_msg:

Static Public Attributes

- tuple pdus

  Dispatch table of PDUs for this protocol.

14.23.1 Detailed Description

Definition at line 226 of file irbe_cli.py.

14.23.2 Member Data Documentation

14.23.2.1 tuple irbe_cli.publication_msg.pdus [static]

Initial value:

```
dict((x.element_name, x)
              for x in (config_elt, client_elt, certificate_elt, crl_elt, manifes
      t_elt, roa_elt, report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented from rpki.publication.msg.

Definition at line 227 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.24 irbe_cli.publication_proto Class Reference

Inherits object.

Collaboration diagram for irbe_cli.publication_proto:

Static Public Attributes

- cms_msg = publication_cms_msg
- msg = publication_msg

14.24.1 Detailed Description

Definition at line 319 of file irbe_cli.py.

14.24.2 Member Data Documentation

14.24.2.1 irbe_cli.publication_proto.cms_msg = publication_cms_msg [static]

Definition at line 321 of file irbe_cli.py.

14.24.2.2 irbe_cli.publication_proto.msg = publication_msg [static]

Definition at line 320 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.25 irbe_cli.publication_sax_handler Class Reference

Inherits rpki::publication::sax_handler.

Collaboration diagram for irbe_cli.publication_sax_handler:

Static Public Attributes

- pdu = publication_msg

14.25.1 Detailed Description

Definition at line 230 of file irbe_cli.py.

14.25.2 Member Data Documentation

14.25.2.1 irbe_cli.publication_sax_handler.pdu = publication_msg [static]

Reimplemented from rpki.publication.sax_handler.

Definition at line 231 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.26 irbe_cli.reply_elt_mixin Class Reference

Inherits object.

Inherited by irbe_cli.cmd_elt_mixin, irbe_cli.report_error_elt, and irbe_cli.report_error_elt.

Collaboration diagram for irbe_cli.reply_elt_mixin:

Public Member Functions

- def client_reply_decode
- def client_reply_show

Static Public Attributes

- is_cmd = False

14.26.1 Detailed Description

```
Protocol mix-in for printout of reply PDUs.
```

Definition at line 52 of file irbe_cli.py.

14.26.2 Member Function Documentation

14.26.2.1 def irbe_cli.reply_elt_mixin.client_reply_decode (*self*)

Reimplemented in irbe_cli.bsc_elt.

Definition at line 59 of file irbe_cli.py.

14.26.2.2 def irbe_cli.reply_elt_mixin.client_reply_show (*self*)

Definition at line 62 of file irbe_cli.py.

14.26.3 Member Data Documentation

14.26.3.1 irbe_cli.reply_elt_mixin.is_cmd = False `[static]`

Reimplemented in irbe_cli.cmd_elt_mixin.

Definition at line 57 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.27 irbe_cli.report_error_elt Class Reference

Inherits irbe_cli::reply_elt_mixin, rpki::publication::report_error_elt, irbe_cli::reply_-elt_mixin, and rpki::left_right::report_error_elt.

Collaboration diagram for irbe_cli.report_error_elt:

14.27.1 Detailed Description

Definition at line 186 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.28 irbe_cli.repository_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::repository_elt.

Collaboration diagram for irbe_cli.repository_elt:

14.28.1 Detailed Description

Definition at line 177 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.29 irbe_cli.roa_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::roa_elt.

Collaboration diagram for irbe_cli.roa_elt:

14.29.1 Detailed Description

Definition at line 220 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.30 irbe_cli.self_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::self_elt.

Collaboration diagram for irbe_cli.self_elt:

14.30.1 Detailed Description

Definition at line 149 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.31 irbe_cli.UsageWrapper Class Reference

Inherits textwrap::TextWrapper.

Collaboration diagram for irbe_cli.UsageWrapper:

Public Member Functions

- def __call__

14.31.1 Detailed Description

```
Call interface around Python textwrap.Textwrapper class.
```

Definition at line 41 of file irbe_cli.py.

14.31.2 Member Function Documentation

14.31.2.1 def irbe_cli.UsageWrapper.__call__ (*self*, *args*)

```
Format arguments, with TextWrapper indentation.
```

Definition at line 46 of file irbe_cli.py.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.32 long Class Reference

Inherited by rpki.ipaddrs.v4addr, and rpki.ipaddrs.v6addr.

The documentation for this class was generated from the following file:

- ipaddrs.py (2424)

14.33 object Class Reference

Inherited by irbe_cli.cmd_msg_mixin, irbe_cli.left_right_proto, irbe_cli.publication_proto, irbe_cli.reply_elt_mixin, pubd.pubd_context, rpki.async.gc_summary, rpki.async.iterator, rpki.async.sync_wrapper, rpki.async.timer, rpki.config.parser, rpki.https.caller, rpki.https.http_message, rpki.https.http_queue, rpki.left_right.left_right_namespace, rpki.log.logger, rpki.myrpki.CA, rpki.myrpki.child, rpki.myrpki.csv_reader, rpki.myrpki.EntityDB, rpki.myrpki.parent, rpki.myrpki.repository, rpki.myrpki.roa_request, rpki.publication.publication_namespace, rpki.resource_set.resource_bag, rpki.resource_set.resource_range, rpki.resource_set.roa_prefix, rpki.rpki_engine.publication_queue, rpki.rpki_engine.rpkid_context, rpki.sql.session, rpki.sql.sql_persistent, rpki.sql.template, rpki.up_down.base_elt, rpki.x509.DeadDrop, rpki.x509.DER_object, rpki.x509.PEM_converter, and rpki.xml_utils.base_elt.

The documentation for this class was generated from the following file:

- x509.py (3107)

14.34 pubd.pubd_context Class Reference

Inherits object.

Collaboration diagram for pubd.pubd_context:

Public Member Functions

- def __init__
- def build_https_ta_cache
- def clear_https_ta_cache

- def client_handler
- def control_handler
- def handler_common

Public Attributes

- bpki_ta
- https_server_host
- https_server_port
- irbe_cert
- pubd_cert
- pubd_key
- publication_base
- publication_multimodule
- sql

Static Public Attributes

- tuple client_url_regexp = re.compile("/client/([-A-Z0-9_/]+)$", re.I)
- https_ta_cache = None

  HTTPS trust anchor cache, to avoid regenerating it for every TLS connection.

14.34.1 Detailed Description

```
A container for various pubd parameters.
```

Definition at line 46 of file pubd.py.

14.34.2 Member Function Documentation

14.34.2.1 def pubd.pubd_context.__init__ (*self*, *cfg*)

Definition at line 51 of file pubd.py.

14.34.2.2 def pubd.pubd_context.build_https_ta_cache (*self*)

```
Build dynamic TLS trust anchors.
```

Definition at line 140 of file pubd.py.

14.34.2.3 def pubd.pubd_context.clear_https_ta_cache (*self*)

```
Clear dynamic TLS trust anchors.
```

Definition at line 132 of file pubd.py.

14.34.2.4 def pubd.pubd_context.client_handler (*self*, *query*, *path*, *cb*)

```
Process one PDU from a client.
```

Definition at line 100 of file pubd.py.

14.34.2.5 def pubd.pubd_context.control_handler (*self*, *query*, *path*, *cb*)

```
Process one PDU from the IRBE.
```

Definition at line 80 of file pubd.py.

14.34.2.6 def pubd.pubd_context.handler_common (*self*, *query*, *client*, *cb*, *certs*, *crl* = `None`)

```
Common PDU handler code.
```

Definition at line 67 of file pubd.py.

14.34.3 Member Data Documentation

14.34.3.1 pubd.pubd_context.bpki_ta

Definition at line 55 of file pubd.py.

14.34.3.2 tuple pubd.pubd_context.client_url_regexp = re.compile("/client/([-A-Z0-9_/]+)$", re.I) [static]

Definition at line 98 of file pubd.py.

14.34.3.3 pubd.pubd_context.https_server_host

Definition at line 60 of file pubd.py.

14.34.3.4 pubd.pubd_context.https_server_port

Definition at line 61 of file pubd.py.

14.34.3.5 pubd.pubd_context::https_ta_cache = None [static]

HTTPS trust anchor cache, to avoid regenerating it for every TLS connection.

Definition at line 130 of file pubd.py.

14.34.3.6 pubd.pubd_context.irbe_cert

Definition at line 56 of file pubd.py.

14.34.3.7 pubd.pubd_context.pubd_cert

Definition at line 57 of file pubd.py.

14.34.3.8 pubd.pubd_context.pubd_key

Definition at line 58 of file pubd.py.

14.34.3.9 pubd.pubd_context.publication_base

Definition at line 63 of file pubd.py.

14.34.3.10 pubd.pubd_context.publication_multimodule

Definition at line 65 of file pubd.py.

14.34.3.11 pubd.pubd_context.sql

Definition at line 53 of file pubd.py.

The documentation for this class was generated from the following file:

- pubd.py (3107)

14.35 datetime Class Reference

Inherited by rpki.sundial.datetime.

The documentation for this class was generated from the following file:

- sundial.py (3191)

14.36 timedelta Class Reference

Inherited by rpki.sundial.timedelta.

The documentation for this class was generated from the following file:

- sundial.py (3191)

14.37 rootd.cms_msg Class Reference

Inherits rpki::up_down::cms_msg.

Collaboration diagram for rootd.cms_msg:

Static Public Attributes

- saxify = sax_handler.saxify

14.37.1 Detailed Description

Definition at line 235 of file rootd.py.

14.37.2 Member Data Documentation

14.37.2.1 rootd.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented from rpki.up_down.cms_msg.

Definition at line 236 of file rootd.py.

The documentation for this class was generated from the following file:

- rootd.py (2913)

14.38 rootd.issue_pdu Class Reference

Inherits rpki::up_down::issue_pdu.

Collaboration diagram for rootd.issue_pdu:

Public Member Functions

- def serve_pdu

14.38.1 Detailed Description

Definition at line 194 of file rootd.py.

14.38.2 Member Function Documentation

14.38.2.1 def rootd.issue_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *callback*, *errback*)

```
Serve one issue request PDU.
```

Reimplemented from rpki.up_down.issue_pdu.

Definition at line 195 of file rootd.py.

The documentation for this class was generated from the following file:

- rootd.py (2913)

14.39 rootd.list_pdu Class Reference

Inherits rpki::up_down::list_pdu.

Collaboration diagram for rootd.list_pdu:

Public Member Functions

- def serve_pdu

14.39.1 Detailed Description

Definition at line 188 of file rootd.py.

14.39.2 Member Function Documentation

14.39.2.1 def rootd.list_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *callback*, *errback*)

```
Serve one "list" PDU.
```

Reimplemented from rpki.up_down.list_pdu.

Definition at line 189 of file rootd.py.

The documentation for this class was generated from the following file:

- rootd.py (2913)

14.40 rootd.message_pdu Class Reference

Inherits rpki::up_down::message_pdu.

Collaboration diagram for rootd.message_pdu:

Public Member Functions

- def log_query

Static Public Attributes

- dictionary name2type

- tuple type2name = dict((v, k) for k, v in name2type.items())

14.40.1 Detailed Description

Definition at line 213 of file rootd.py.

14.40.2 Member Function Documentation

14.40.2.1 def rootd.message_pdu.log_query (*self*, *child*)

```
Log query we're handling.
```

Reimplemented from rpki.up_down.message_pdu.

Definition at line 226 of file rootd.py.

14.40.3 Member Data Documentation

14.40.3.1 dictionary rootd.message_pdu.name2type [static]

Initial value:

```
{
    "list"            : list_pdu,
    "list_response"   : rpki.up_down.list_response_pdu,
    "issue"           : issue_pdu,
    "issue_response"  : rpki.up_down.issue_response_pdu,
    "revoke"          : revoke_pdu,
    "revoke_response" : rpki.up_down.revoke_response_pdu,
    "error_response"  : rpki.up_down.error_response_pdu }
```

Reimplemented from rpki.up_down.message_pdu.

Definition at line 215 of file rootd.py.

14.40.3.2 tuple rootd.message_pdu.type2name = dict((v, k) for k, v in name2type.items()) [static]

Reimplemented from rpki.up_down.message_pdu.

Definition at line 224 of file rootd.py.

The documentation for this class was generated from the following file:

- rootd.py (2913)

14.41 rootd.revoke_pdu Class Reference

Inherits rpki::up_down::revoke_pdu.

Collaboration diagram for rootd.revoke_pdu:

Public Member Functions

- def serve_pdu

14.41.1 Detailed Description

Definition at line 201 of file rootd.py.

14.41.2 Member Function Documentation

14.41.2.1 def rootd.revoke_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *cb*, *eb*)

```
Serve one revoke request PDU.
```

Reimplemented from rpki.up_down.revoke_pdu.

Definition at line 202 of file rootd.py.

The documentation for this class was generated from the following file:

- rootd.py (2913)

14.42 rootd.sax_handler Class Reference

Inherits rpki::up_down::sax_handler.

Collaboration diagram for rootd.sax_handler:

Static Public Attributes

- pdu = message_pdu

14.42.1 Detailed Description

Definition at line 232 of file rootd.py.

14.42.2 Member Data Documentation

14.42.2.1 rootd.sax_handler.pdu = message_pdu [static]

Reimplemented from rpki.up_down.sax_handler.

Definition at line 233 of file rootd.py.

The documentation for this class was generated from the following file:

- rootd.py (2913)

14.43 rpki.async.gc_summary Class Reference

Inherits object.

Collaboration diagram for rpki.async.gc_summary:

Public Member Functions

- def __init__

- def handler

Public Attributes

- interval
- threshold
- timer

14.43.1 Detailed Description

```
Periodic summary of GC state, for tracking down memory bloat.
```

Definition at line 368 of file async.py.

14.43.2 Member Function Documentation

14.43.2.1 def rpki.async.gc_summary.__init__ (*self*, *interval*, *threshold* = 0)

Definition at line 373 of file async.py.

14.43.2.2 def rpki.async.gc_summary.handler (*self*)

```
Collect and log GC state for this period, reset timer.
```

Definition at line 381 of file async.py.

14.43.3 Member Data Documentation

14.43.3.1 rpki.async.gc_summary.interval

Definition at line 376 of file async.py.

14.43.3.2 rpki.async.gc_summary.threshold

Definition at line 377 of file async.py.

14.43.3.3 rpki.async.gc_summary.timer

Definition at line 378 of file async.py.

The documentation for this class was generated from the following file:

- async.py (3191)

14.44 rpki.async.iterator Class Reference

Inherits object.

Collaboration diagram for rpki.async.iterator:

Public Member Functions

- def __call__
- def __init__
- def __repr__
- def doit

Public Attributes

- caller_function
- done_callback
- item_callback
- iterator
- unwind_stack

14.44.1 Detailed Description

```
Iteration construct for event-driven code.  Takes three
arguments:

- Some kind of iterable object

- A callback to call on each item in the iteration

- A callback to call after the iteration terminates.

The item callback receives two arguments: the callable iterator
object and the current value of the iteration.  It should call the
iterator (or arrange for the iterator to be called) when it is time
to continue to the next item in the iteration.

The termination callback receives no arguments.
```

Definition at line 26 of file async.py.

14.44.2 Member Function Documentation

14.44.2.1 def rpki.async.iterator.__call__ (*self*)

Definition at line 64 of file async.py.

14.44.2.2 def rpki.async.iterator.__init__ (*self*, *iterable*, *item_callback*, *done_callback*, *unwind_stack* = `True`)

Definition at line 45 of file async.py.

14.44.2.3 def rpki.async.iterator.__repr__ (*self*)

Definition at line 59 of file async.py.

14.44.2.4 def rpki.async.iterator.doit (*self*)

```
Implement the iterator protocol: attempt to call the item handler
with the next iteration value, call the termination handler if the
iterator signaled StopIteration.
```

Definition at line 70 of file async.py.

14.44.3 Member Data Documentation

14.44.3.1 rpki.async.iterator.caller_function

Definition at line 48 of file async.py.

14.44.3.2 rpki.async.iterator.done_callback

Definition at line 47 of file async.py.

14.44.3.3 rpki.async.iterator.item_callback

Definition at line 46 of file async.py.

14.44.3.4 rpki.async.iterator.iterator

Definition at line 51 of file async.py.

14.44.3.5 rpki.async.iterator.unwind_stack

Definition at line 49 of file async.py.

The documentation for this class was generated from the following file:

- async.py (3191)

14.45 rpki.async.sync_wrapper Class Reference

Inherits object.

Collaboration diagram for rpki.async.sync_wrapper:

Public Member Functions

- def __call__
- def __init__
- def cb
- def eb

Public Attributes

- func

Static Public Attributes

- err = None
- res = None

14.45.1 Detailed Description

```
Synchronous wrapper around asynchronous functions.  Running in
asynchronous mode at all times makes sense for event-driven daemons,
but is kind of tedious for simple scripts, hence this wrapper.

The wrapped function should take at least two arguments: a callback
function and an errback function.  If any arguments are passed to
the wrapper, they will be passed as additional arguments to the
wrapped function.
```

Definition at line 305 of file async.py.

14.45.2 Member Function Documentation

14.45.2.1 def rpki.async.sync_wrapper.__call__ (*self*, *args*, *kwargs*)

Definition at line 340 of file async.py.

14.45.2.2 def rpki.async.sync_wrapper.__init__ (*self*, *func*)

Definition at line 320 of file async.py.

14.45.2.3 def rpki.async.sync_wrapper.cb (*self*, *res* = `None`)

```
Wrapped code has requested normal termination.  Store result, and
exit the event loop.
```

Definition at line 323 of file async.py.

14.45.2.4 def rpki.async.sync_wrapper.eb (*self*, *err*)

```
Wrapped code raised an exception.  Store exception data, then exit
the event loop.
```

Definition at line 331 of file async.py.

14.45.3 Member Data Documentation

14.45.3.1 rpki.async.sync_wrapper.err = None [static]

Definition at line 318 of file async.py.

14.45.3.2 rpki.async.sync_wrapper.func

Definition at line 321 of file async.py.

14.45.3.3 rpki.async.sync_wrapper.res = None [static]

Definition at line 317 of file async.py.

The documentation for this class was generated from the following file:

- async.py (3191)

14.46 rpki.async.timer Class Reference

Inherits object.

Collaboration diagram for rpki.async.timer:

Public Member Functions

- def __cmp__
- def __del__
- def __init__
- def __repr__
- def cancel

- def clear
- def errback
- def handler
- def is_set
- def runq
- def seconds_until_wakeup
- def set
- def set_errback
- def set_handler
- def trace

Public Attributes

- errback
- handler
- when

Static Public Attributes

- gc_debug = False

  Verbose chatter about timers states and garbage collection.

- list queue = [ ]

  Timer queue, shared by all timer instances (there can be only one queue).

- run_debug = False

  Verbose chatter about timers being run.

14.46.1 Detailed Description

```
Timer construct for event-driven code.  It can be used in either of two ways:

- As a virtual class, in which case the subclass should provide a
  handler() method to receive the wakup event when the timer expires; or

- By setting an explicit handler callback, either via the
  constructor or the set_handler() method.

Subclassing is probably more Pythonic, but setting an explict
handler turns out to be very convenient when combined with bound
methods to other objects.
```

Definition at line 82 of file async.py.

14.46.2 Member Function Documentation

14.46.2.1 def rpki.async.timer.__cmp__ (*self*, *other*)

Definition at line 142 of file async.py.

14.46.2.2 def rpki.async.timer.__del__ (*self*)

Definition at line 146 of file async.py.

14.46.2.3 def rpki.async.timer.__init__ (*self*, *handler* = `None`, *errback* = `None`)

Definition at line 109 of file async.py.

14.46.2.4 def rpki.async.timer.__repr__ (*self*)

Definition at line 209 of file async.py.

14.46.2.5 def rpki.async.timer.cancel (*self*)

```
Cancel a timer, if it was set.
```

Definition at line 149 of file async.py.

14.46.2.6 def rpki.async.timer.clear (*cls*)

```
Cancel every timer on the queue.  We could just throw away the
queue content, but this way we can notify subclasses that provide
their own cancel() method.
```

Definition at line 234 of file async.py.

14.46.2.7 def rpki.async.timer.errback (*self*, *e*)

```
Error callback.  May be overridden, or set with set_errback().
```

Definition at line 181 of file async.py.

14.46.2.8 def rpki.async.timer.handler (*self*)

```
Handle a timer that has expired.  This must either be overriden by
a subclass or set dynamically by set_handler().
```

Definition at line 164 of file async.py.

14.46.2.9 def rpki.async.timer.is_set (*self*)

```
Test whether this timer is currently set.
```

Definition at line 160 of file async.py.

14.46.2.10 def rpki.async.timer.runq (*cls*)

```
Run the timer queue: for each timer whose call time has passed,
pull the timer off the queue and call its handler() method.
```

Definition at line 193 of file async.py.

14.46.2.11 def rpki.async.timer.seconds_until_wakeup (*cls*)

```
Calculate delay until next timer expires, or None if no timers are
set and we should wait indefinitely.  Rounds up to avoid spinning
in select() or poll().  We could calculate fractional seconds in
the right units instead, but select() and poll() don't even take
the same units (argh!), and we're not doing anything that
hair-triggered, so rounding up is simplest.
```

Definition at line 213 of file async.py.

14.46.2.12 def rpki.async.timer.set (*self*, *when*)

```
Set a timer.  Argument can be a datetime, to specify an absolute
time, or a timedelta, to specify an offset time.
```

Definition at line 126 of file async.py.

14.46.2.13 def rpki.async.timer.set_errback (*self*, *errback*)

```
Set a timer's errback.  Like set_handler(), for errbacks.
```

Definition at line 188 of file async.py.

14.46.2.14 def rpki.async.timer.set_handler (*self*, *handler*)

```
Set timer's expiration handler.  This is an alternative to
subclassing the timer class, and may be easier to use when
integrating timers into other classes (eg, the handler can be a
bound method to an object in a class representing a network
connection).
```

Definition at line 171 of file async.py.

14.46.2.15 def rpki.async.timer.trace (*self*, *msg*)

```
Debug logging.
```

Definition at line 118 of file async.py.

14.46.3 Member Data Documentation

14.46.3.1 rpki.async.timer.errback

Definition at line 190 of file async.py.

14.46.3.2 rpki::async.timer::gc_debug = False [static]

Verbose chatter about timers states and garbage collection.

Definition at line 99 of file async.py.

14.46.3.3 rpki.async.timer.handler

Definition at line 179 of file async.py.

14.46.3.4 rpki::async.timer::queue = [] [static]

Timer queue, shared by all timer instances (there can be only one queue).

Definition at line 107 of file async.py.

14.46.3.5 rpki::async.timer::run_debug = False [static]

Verbose chatter about timers being run.

Definition at line 103 of file async.py.

14.46.3.6 rpki.async.timer.when

Definition at line 114 of file async.py.

The documentation for this class was generated from the following file:

- async.py (3191)

14.47 rpki.cli.Cmd Class Reference

Inherits cmd::Cmd.

Inherited by rpki.myrpki.main.

Collaboration diagram for rpki.cli.Cmd:

Public Member Functions

- def __init__
- def cmdloop_with_history
- def complete_help
- def completenames

- def do_EOF
- def do_exit
- def emptyline
- def filename_complete
- def help_help
- def onecmd

Static Public Attributes

- cmdloop_with_history = cmd.Cmd.cmdloop
- do_quit = do_exit
- emptyline_repeats_last_command = False
- EOF_exits_command_loop = True
- histfile = None
- string identchars = "/-."

14.47.1 Detailed Description

```
Customized subclass of Python cmd module.
```

Definition at line 29 of file cli.py.

14.47.2 Member Function Documentation

14.47.2.1 def rpki.cli.Cmd.__init__ (*self*, *argv* = `None`)

Definition at line 42 of file cli.py.

14.47.2.2 def rpki.cli.Cmd.cmdloop_with_history (*self*)

```
Better command loop, with history file and tweaked readline
completion delimiters.
```

Definition at line 132 of file cli.py.

14.47.2.3 def rpki.cli.Cmd.complete_help (*self*, *args*)

```
Better completion function for help command arguments.
```

Definition at line 119 of file cli.py.

14.47.2.4 def rpki.cli.Cmd.completenames (*self*, *text*, *ignored*)

```
Command name completion handler, with hack to restore what I
consider the normal (bash-like) behavior when one hits the
completion key and there's only one match.
```

Definition at line 101 of file cli.py.

14.47.2.5 def rpki.cli.Cmd.do_EOF (*self*, *arg*)

```
Exit program.
```

Definition at line 61 of file cli.py.

14.47.2.6 def rpki.cli.Cmd.do_exit (*self*, *arg*)

```
Exit program.
```

Definition at line 69 of file cli.py.

14.47.2.7 def rpki.cli.Cmd.emptyline (*self*)

```
Handle an empty line.  cmd module default is to repeat the last
command, which I find to be violation of the principal of least
astonishment, so my preference is that an empty line does nothing.
```

Definition at line 77 of file cli.py.

14.47.2.8 def rpki.cli.Cmd.filename_complete (*self*, *text*, *line*, *begidx*, *endidx*)

```
Filename completion handler, with hack to restore what I consider
the normal (bash-like) behavior when one hits the completion key
and there's only one match.
```

Definition at line 86 of file cli.py.

14.47.2.9 def rpki.cli.Cmd.help_help (*self*)

```
Type "help [topic]" for help on a command,
or just "help" for a list of commands.
```

Definition at line 112 of file cli.py.

14.47.2.10 def rpki.cli.Cmd.onecmd (*self*, *line*)

```
Wrap error handling around cmd.Cmd.onecmd().  Might want to do
something kinder than showing a traceback, eventually.
```

Definition at line 49 of file cli.py.

14.47.3 Member Data Documentation

14.47.3.1 rpki.cli.Cmd.cmdloop_with_history = cmd.Cmd.cmdloop [static]

Definition at line 153 of file cli.py.

14.47.3.2 rpki.cli.Cmd.do_quit = do_exit [static]

Definition at line 75 of file cli.py.

14.47.3.3 rpki.cli.Cmd.emptyline_repeats_last_command = False [static]

Definition at line 34 of file cli.py.

14.47.3.4 rpki.cli.Cmd.EOF_exits_command_loop = True [static]

Definition at line 36 of file cli.py.

14.47.3.5 rpki.cli.Cmd.histfile = None [static]

Reimplemented in rpki.myrpki.main.

Definition at line 40 of file cli.py.

14.47.3.6 string rpki.cli.Cmd.identchars = "/-." [static]

Definition at line 38 of file cli.py.

The documentation for this class was generated from the following file:

- cli.py (3191)

14.48 rpki.config.parser Class Reference

Inherits object.

Collaboration diagram for rpki.config.parser:

Public Member Functions

- def __init__
- def get
- def getboolean
- def getint

- def getlong
- def has_option
- def has_section
- def multiget
- def set_global_flags

Public Attributes

- cfg
- default_section
- filename

Private Member Functions

- def _repl

Static Private Attributes

- tuple _regexp = re.compile("\\${(.*?)::(.*?)}")

14.48.1 Detailed Description

```
Extensions to stock Python ConfigParser:

Read config file and set default section while initializing parser object.

Support for OpenSSL-style subscripted options and a limited form of
OpenSSL-style indirect variable references (${section::option}).

get-methods with default values and default section name.
```

Definition at line 38 of file config.py.

14.48.2 Member Function Documentation

14.48.2.1 def rpki.config.parser.__init__ (*self*, *filename*, *section* = `None`, *allow_missing* = `False`)

```
Initialize this parser.
```

Definition at line 50 of file config.py.

14.48.2.2 def rpki.config.parser._repl (*self*, *m*) [private]

```
Replacement function for indirect variable substitution.
This is intended for use with re.subn().
```

Definition at line 101 of file config.py.

14.48.2.3 def rpki.config.parser.get (*self*, *option*, *default* = None, *section* = None)

```
Get an option, perhaps with a default value.
```

Definition at line 112 of file config.py.

14.48.2.4 def rpki.config.parser.getboolean (*self*, *option*, *default* = None, *section* = None)

```
Get a boolean option, perhaps with a default value.
```

Definition at line 126 of file config.py.

14.48.2.5 def rpki.config.parser.getint (*self*, *option*, *default* = None, *section* = None)

```
Get an integer option, perhaps with a default value.
```

Definition at line 138 of file config.py.

14.48.2.6 def rpki.config.parser.getlong (*self*, *option*, *default* = None, *section* = None)

```
Get a long integer option, perhaps with a default value.
```

Definition at line 144 of file config.py.

14.48.2.7 def rpki.config.parser.has_option (*self*, *option*, *section* = `None`)

```
Test whether an option exists.
```

Definition at line 71 of file config.py.

14.48.2.8 def rpki.config.parser.has_section (*self*, *section*)

```
Test whether a section exists.
```

Definition at line 64 of file config.py.

14.48.2.9 def rpki.config.parser.multiget (*self*, *option*, *section* = `None`)

```
Parse OpenSSL-style foo.0, foo.1, ... subscripted options.

Returns a list of values matching the specified option name.
```

Definition at line 80 of file config.py.

14.48.2.10 def rpki.config.parser.set_global_flags (*self*)

```
Consolidated control for all the little global control flags
scattered through the libraries.  This isn't a particularly good
place for this function to live, but it has to live somewhere and
making it a method of the config parser from which it gets all of
its data is less silly than the available alternatives.
```

Definition at line 150 of file config.py.

14.48.3 Member Data Documentation

14.48.3.1 tuple rpki.config.parser._regexp = re.compile("\\${(.*?)::(.*?)}") `[static, private]`

Definition at line 99 of file config.py.

14.48.3.2 rpki.config.parser.cfg

Definition at line 56 of file config.py.

14.48.3.3 rpki.config.parser.default_section

Definition at line 62 of file config.py.

14.48.3.4 rpki.config.parser.filename

Definition at line 55 of file config.py.

The documentation for this class was generated from the following file:

- config.py (3107)

14.49 rpki.exceptions.BadClassNameSyntax Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadClassNameSyntax:

14.49.1 Detailed Description

```
Illegal syntax for a class_name.
```

Definition at line 92 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.50 rpki.exceptions.BadClientURL Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadClientURL:

14.50.1 Detailed Description

```
URL given to HTTPS client does not match profile.
```

Definition at line 232 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.51 rpki.exceptions.BadContactURL Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadContactURL:

14.51.1 Detailed Description

```
Error trying to parse contact URL.
```

Definition at line 87 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.52 rpki.exceptions.BadExtension Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadExtension:

14.52.1 Detailed Description

```
Forbidden X.509 extension.
```

Definition at line 242 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.53 rpki.exceptions.BadIRDBReply Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadIRDBReply:

14.53.1 Detailed Description

```
Unexpected reply to IRDB query.
```

Definition at line 152 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.54 rpki.exceptions.BadIssueResponse Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadIssueResponse:

14.54.1 Detailed Description

```
issue_response PDU with wrong number of classes or certificates.
```

Definition at line 97 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.55 rpki.exceptions.BadPKCS10 Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadPKCS10:

14.55.1 Detailed Description

```
Bad PKCS #10 object.
```

Definition at line 107 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.56 rpki.exceptions.BadPublicationReply Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadPublicationReply:

14.56.1 Detailed Description

```
Unexpected reply to publication query.
```

Definition at line 257 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.57 rpki.exceptions.BadQuery Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadQuery:

14.57.1 Detailed Description

```
Unexpected protocol query.
```

Definition at line 55 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.58 rpki.exceptions.BadSender Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadSender:

14.58.1 Detailed Description

```
Unexpected XML sender value.
```

Definition at line 127 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.59 rpki.exceptions.BadStatusCode Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadStatusCode:

14.59.1 Detailed Description

```
Unrecognized protocol status code.
```

Definition at line 50 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.60 rpki.exceptions.BadURISyntax Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BadURISyntax:

14.60.1 Detailed Description

```
Illegal syntax for a URI.
```

Definition at line 45 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.61 rpki.exceptions.BSCNotFound Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BSCNotFound:

14.61.1 Detailed Description

```
Could not find specified BSC in database.
```

Definition at line 122 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.62 rpki.exceptions.BSCNotReady Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.BSCNotReady:

14.62.1 Detailed Description

```
BSC not yet in a usable state, signing_cert not set.
```

Definition at line 277 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.63 rpki.exceptions.ChildNotFound Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.ChildNotFound:

14.63.1 Detailed Description

```
Could not find specified child in database.
```

Definition at line 117 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.64 rpki.exceptions.ClassNameMismatch Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.ClassNameMismatch:

14.64.1 Detailed Description

```
class_name does not match child context.
```

Definition at line 132 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.65 rpki.exceptions.ClassNameUnknown Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.ClassNameUnknown:

14.65.1 Detailed Description

```
Unknown class_name.
```

Definition at line 137 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.66 rpki.exceptions.ClientNotFound Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.ClientNotFound:

14.66.1 Detailed Description

```
Could not find specified client in database.
```

Definition at line 237 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.67 rpki.exceptions.CMSContentNotSet Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.CMSContentNotSet:

14.67.1 Detailed Description

```
Inner content of a CMS_object has not been set.  If object is known
to be valid, the .extract() method should be able to set the
content; otherwise, only the .verify() method (which checks
signatures) is safe.
```

Definition at line 302 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.68 rpki.exceptions.CMSCRLNotSet Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.CMSCRLNotSet:

14.68.1 Detailed Description

```
CMS CRL has not been configured.
```

Definition at line 217 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.69 rpki.exceptions.CMSVerificationFailed Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.CMSVerificationFailed:

14.69.1 Detailed Description

```
Verification of a CMS message failed.
```

Definition at line 66 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.70 rpki.exceptions.DBConsistancyError Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.DBConsistancyError:

14.70.1 Detailed Description

```
Found multiple matches for a database query that shouldn't ever
return that.
```

Definition at line 60 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.71 rpki.exceptions.DERObjectConversionError Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.DERObjectConversionError:

14.71.1 Detailed Description

```
Error trying to convert a DER-based object from one representation
to another.
```

Definition at line 76 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.72 rpki.exceptions.DuplicateObject Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.DuplicateObject:

14.72.1 Detailed Description

```
Attempt to create an object that already exists.
```

Definition at line 262 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.73 rpki.exceptions.EmptyPEM Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.EmptyPEM:

14.73.1 Detailed Description

```
Couldn't find PEM block to convert.
```

Definition at line 187 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.74 rpki.exceptions.EmptyROAPrefixList Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.EmptyROAPrefixList:

14.74.1 Detailed Description

```
Can't create ROA with an empty prefix list.
```

Definition at line 267 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.75 rpki.exceptions.ForbiddenURI Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.ForbiddenURI:

14.75.1 Detailed Description

```
Forbidden URI, does not start with correct base URI.
```

Definition at line 247 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.76 rpki.exceptions.HandleTranslationError Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.HandleTranslationError:

14.76.1 Detailed Description

```
Internal error translating protocol handle -> SQL id.
```

Definition at line 292 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.77 rpki.exceptions.HTTPRequestFailed Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.HTTPRequestFailed:

14.77.1 Detailed Description

```
HTTP request failed.
```

Definition at line 71 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.78 rpki.exceptions.HTTPSBadVersion Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.HTTPSBadVersion:

14.78.1 Detailed Description

```
HTTPS couldn't parse HTTP version.
```

Definition at line 287 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.79 rpki.exceptions.HTTPSClientAborted Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.HTTPSClientAborted:

14.79.1 Detailed Description

```
HTTPS client connection closed while in request-sent state.
```

Definition at line 252 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.80 rpki.exceptions.HTTPSUnexpectedState Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.HTTPSUnexpectedState:

14.80.1 Detailed Description

```
HTTPS event occurred in an unexpected state.
```

Definition at line 282 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.81 rpki.exceptions.MissingCMSCRL Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.MissingCMSCRL:

14.81.1 Detailed Description

```
Didn't receive CMS CRL when expecting one.
```

Definition at line 207 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.82 rpki.exceptions.MissingCMSEEcert Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.MissingCMSEEcert:

14.82.1 Detailed Description

```
Didn't receive CMS EE cert when expecting one.
```

Definition at line 202 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.83 rpki.exceptions.MultipleTLSEECert Class Reference

Inherits rpki::exceptions::TLSValidationError.

Collaboration diagram for rpki.exceptions.MultipleTLSEECert:

14.83.1 Detailed Description

```
Received more than one TLS EE certificate.
```

Definition at line 172 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.84 rpki.exceptions.MustBePrefix Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.MustBePrefix:

14.84.1 Detailed Description

```
Resource range cannot be expressed as a prefix.
```

Definition at line 162 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.85 rpki.exceptions.NoActiveCA Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.NoActiveCA:

14.85.1 Detailed Description

```
No active ca_detail for specified class.
```

Definition at line 227 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.86 rpki.exceptions.NoCoveringCertForROA Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.NoCoveringCertForROA:

14.86.1 Detailed Description

```
Couldn't find a covering certificate to generate ROA.
```

Definition at line 272 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.87 rpki.exceptions.NoObjectAtURI Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.NoObjectAtURI:

14.87.1 Detailed Description

```
No object published at specified URI.
```

Definition at line 297 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.88 rpki.exceptions.NotACertificateChain Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.NotACertificateChain:

14.88.1 Detailed Description

```
Certificates don't form a proper chain.
```

Definition at line 82 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.89 rpki.exceptions.NotFound Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.NotFound:

14.89.1 Detailed Description

```
Object not found in database.
```

Definition at line 157 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.90 rpki.exceptions.NotImplementedYet Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.NotImplementedYet:

14.90.1 Detailed Description

```
Internal error -- not implemented yet.
```

Definition at line 102 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.91 rpki.exceptions.NotInDatabase Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.NotInDatabase:

14.91.1 Detailed Description

```
Lookup failed for an object expected to be in the database.
```

Definition at line 40 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.92 rpki.exceptions.ReceivedTLSCACert Class Reference

Inherits rpki::exceptions::TLSValidationError.

Collaboration diagram for rpki.exceptions.ReceivedTLSCACert:

14.92.1 Detailed Description

`Received CA certificate via TLS.`

Definition at line 177 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.93 rpki.exceptions.RPKI_Exception Class Reference

Inherits Exception.

Inherited by rpki.exceptions.BadClassNameSyntax, rpki.exceptions.BadClientURL, rpki.exceptions.BadContactURL, rpki.exceptions.BadExtension, rpki.exceptions.BadIRDBReply, rpki.exceptions.BadIssueResponse, rpki.exceptions.BadPKCS10, rpki.exceptions.BadPublicationReply, rpki.exceptions.BadQuery, rpki.exceptions.BadSender, rpki.exceptions.BadStatusCode, rpki.exceptions.BadURISyntax, rpki.exceptions.BSCNotFound, rpki.exceptions.BSCNotReady, rpki.exceptions.ChildNotFound, rpki.exceptions.ClassNameMismatch, rpki.exceptions.ClassNameUnknown, rpki.exceptions.ClientNotFound, rpki.exceptions.CMSContentNotSet, rpki.exceptions.CMSCRLNotSet, rpki.exceptions.CMSVerificationFailed, rpki.exceptions.DBConsistancyError, rpki.exceptions.DERObjectConversionError, rpki.exceptions.DuplicateObject, rpki.exceptions.EmptyPEM, rpki.exceptions.EmptyROAPrefixList, rpki.exceptions.ForbiddenURI, rpki.exceptions.HandleTranslationError, rpki.exceptions.HTTPRequestFailed, rpki.exceptions.HTTPSBadVersion, rpki.exceptions.HTTPSClientAborted, rpki.exceptions.HTTPSUnexpectedState, rpki.exceptions.MissingCMSCRL, rpki.exceptions.MissingCMSEEcert, rpki.exceptions.MustBePrefix, rpki.exceptions.NoActiveCA, rpki.exceptions.NoCoveringCertForROA, rpki.exceptions.NoObjectAtURI, rpki.exceptions.NotACertificateChain, rpki.exceptions.NotFound, rpki.exceptions.NotImplementedYet, rpki.exceptions.NotInDatabase, rpki.exceptions.ServerShuttingDown, rpki.exceptions.SKIMismatch, rpki.exceptions.SubprocessError, rpki.exceptions.TLSValidationError, rpki.exceptions.UnexpectedCMSCerts, rpki.exceptions.UnexpectedCMSCRLs, rpki.exceptions.UnparsableCMSDER, rpki.exceptions.UpstreamError, and rpki.exceptions.WrongEContentType.

Collaboration diagram for rpki.exceptions.RPKI_Exception:

14.93.1 Detailed Description

```
Base class for RPKI exceptions.
```

Definition at line 35 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.94 rpki.exceptions.ServerShuttingDown Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.ServerShuttingDown:

14.94.1 Detailed Description

```
Server is shutting down.
```

Definition at line 222 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.95 rpki.exceptions.SKIMismatch Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.SKIMismatch:

14.95.1 Detailed Description

```
SKI value in response does not match request.
```

Definition at line 142 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.96 rpki.exceptions.SubprocessError Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.SubprocessError:

14.96.1 Detailed Description

```
Subprocess returned unexpected error.
```

Definition at line 147 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.97 rpki.exceptions.TLSValidationError Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Inherited by rpki.exceptions.MultipleTLSEECert, and rpki.exceptions.ReceivedTLSCACert.

Collaboration diagram for rpki.exceptions.TLSValidationError:

14.97.1 Detailed Description

```
TLS certificate validation error.
```

Definition at line 167 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.98 rpki.exceptions.UnexpectedCMSCerts Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.UnexpectedCMSCerts:

14.98.1 Detailed Description

```
Received CMS certs when not expecting any.
```

Definition at line 192 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.99 rpki.exceptions.UnexpectedCMSCRLs Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.UnexpectedCMSCRLs:

14.99.1 Detailed Description

```
Received CMS CRLs when not expecting any.
```

Definition at line 197 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.100 rpki.exceptions.UnparsableCMSDER Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.UnparsableCMSDER:

14.100.1 Detailed Description

```
Alleged CMS DER wasn't parsable.
```

Definition at line 212 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.101 rpki.exceptions.UpstreamError Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.UpstreamError:

14.101.1 Detailed Description

```
Received an error from upstream.
```

Definition at line 112 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.102 rpki.exceptions.WrongEContentType Class Reference

Inherits rpki::exceptions::RPKI_Exception.

Collaboration diagram for rpki.exceptions.WrongEContentType:

14.102.1 Detailed Description

```
Received wrong CMS eContentType.
```

Definition at line 182 of file exceptions.py.

The documentation for this class was generated from the following file:

- exceptions.py (2907)

14.103 rpki.https.caller Class Reference

Inherits object.

Collaboration diagram for rpki.https.caller:

Public Member Functions

- def __call__
- def __init__

Public Attributes

- client_cert

- client_key
- proto
- server_cert
- server_ta
- url

Static Public Attributes

- debug = False

14.103.1 Detailed Description

```
Handle client-side mechanics for protocols based on HTTPS, CMS, and
rpki.xml_utils.  Calling sequence is intended to nest within
rpki.async.sync_wrapper.
```

Definition at line 1105 of file https.py.

14.103.2 Member Function Documentation

14.103.2.1 def rpki.https.caller.__call__ (*self*, *cb*, *eb*, *pdus*)

Definition at line 1124 of file https.py.

14.103.2.2 def rpki.https.caller.__init__ (*self*, *proto*, *client_key*, *client_cert*, *server_ta*, *server_cert*, *url*, *debug* = `None`)

Definition at line 1114 of file https.py.

14.103.3 Member Data Documentation

14.103.3.1 rpki.https.caller.client_cert

Definition at line 1117 of file https.py.

14.103.3.2 rpki.https.caller.client_key

Definition at line 1116 of file https.py.

14.103.3.3 rpki.https.caller.debug = False [static]

Definition at line 1112 of file https.py.

14.103.3.4 rpki.https.caller.proto

Definition at line 1115 of file https.py.

14.103.3.5 rpki.https.caller.server_cert

Definition at line 1119 of file https.py.

14.103.3.6 rpki.https.caller.server_ta

Definition at line 1118 of file https.py.

14.103.3.7 rpki.https.caller.url

Definition at line 1120 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

14.104 rpki.https.http_client Class Reference

Inherits rpki::https::http_stream.

Collaboration diagram for rpki.https.http_client:

Public Member Functions

- def __init__
- def handle_close
- def handle_connect
- def handle_error
- def handle_message

- def handle_no_content_length
- def handle_timeout
- def send_request
- def set_state
- def start
- def tls_connect

Public Attributes

- af
- cert
- expect_close
- hostport
- key
- queue
- retry_read
- retry_write
- state
- ta
- tls

Static Public Attributes

- parse_type = http_response

  Stream parser should look for incoming HTTP response messages.

- timeout = default_client_timeout

  Use the default client timeout value set in the module header.

14.104.1 Detailed Description

```
HTTP(S) client stream.
```

Definition at line 759 of file https.py.

14.104.2 Member Function Documentation

14.104.2.1 def rpki.https.http_client.__init__ (*self*, *queue*, *hostport*, *cert* = `None`, *key* = `None`, *ta* = `()`, *af* = supported_address_families`[0]`)

Definition at line 772 of file https.py.

14.104.2.2 def rpki.https.http_client.handle_close (*self*)

```
Asyncore signaled connection close.  If we were waiting for that
to find the end of a response message, process the resulting
message now; if we were waiting for the response to a request we
sent, signal the error.
```

Reimplemented from rpki.https.http_stream.

Definition at line 892 of file https.py.

14.104.2.3 def rpki.https.http_client.handle_connect (*self*)

```
Asyncore says socket has connected, configure TLS junk.
```

Definition at line 797 of file https.py.

14.104.2.4 def rpki.https.http_client.handle_error (*self*)

```
Asyncore says something threw an exception.  Log it, then shut
down the connection and pass back the exception.
```

Reimplemented from rpki.https.http_stream.

Definition at line 918 of file https.py.

14.104.2.5 def rpki.https.http_client.handle_message (*self*)

```
Handle incoming HTTP response message.  Make sure we're in a state
where we expect to see such a message (and allow the mysterious
empty messages that Apache sends during connection close, no idea
what that is supposed to be about).  If everybody agrees that the
connection should stay open, put it into an idle state; otherwise,
arrange for the stream to shut down.
```

Definition at line 856 of file https.py.

14.104.2.6 def rpki.https.http_client.handle_no_content_length (*self*)

```
Handle response message that used neither chunking nor a
Content-Length header (that is: this message will be the last one
in this server stream).  In this case we want to read until we
reach the end of the data stream.
```

Definition at line 836 of file https.py.

14.104.2.7 def rpki.https.http_client.handle_timeout (*self*)

```
Connection idle timer has expired.  If we weren't idle, log that
something bad has happened, then shut down the connection in any
case.
```

Reimplemented from rpki.https.http_stream.

Definition at line 907 of file https.py.

14.104.2.8 def rpki.https.http_client.send_request (*self*, *msg*)

```
Queue up request message and kickstart connection.
```

Definition at line 845 of file https.py.

14.104.2.9 def rpki.https.http_client.set_state (*self*, *state*)

```
Set HTTP client connection state.
```

Definition at line 829 of file https.py.

14.104.2.10 def rpki.https.http_client.start (*self*)

```
Create socket and request a connection.
```

Definition at line 785 of file https.py.

14.104.2.11 def rpki.https.http_client.tls_connect (*self*)

```
Initialize client side of TLS.
```

Definition at line 814 of file https.py.

14.104.3 Member Data Documentation

14.104.3.1 rpki.https.http_client.af

Definition at line 783 of file https.py.

14.104.3.2 rpki.https.http_client.cert

Definition at line 780 of file https.py.

14.104.3.3 rpki.https.http_client.expect_close

Definition at line 779 of file https.py.

14.104.3.4 rpki.https.http_client.hostport

Definition at line 777 of file https.py.

14.104.3.5 rpki.https.http_client.key

Definition at line 781 of file https.py.

14.104.3.6 rpki::https.http_client::parse_type = http_response [static]

Stream parser should look for incoming HTTP response messages.

Definition at line 766 of file https.py.

14.104.3.7 rpki.https.http_client.queue

Definition at line 776 of file https.py.

14.104.3.8 rpki.https.http_client.retry_read

Reimplemented from rpki.https.http_stream.

Definition at line 821 of file https.py.

14.104.3.9 rpki.https.http_client.retry_write

Reimplemented from rpki.https.http_stream.

Definition at line 823 of file https.py.

14.104.3.10 rpki.https.http_client.state

Definition at line 778 of file https.py.

14.104.3.11 rpki.https.http_client.ta

Definition at line 782 of file https.py.

14.104.3.12 rpki::https.http_client::timeout = default_client_timeout [static]

Use the default client timeout value set in the module header.

Definition at line 770 of file https.py.

14.104.3.13 rpki.https.http_client.tls

Reimplemented from rpki.https.http_stream.

Definition at line 802 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

14.105 rpki.https.http_listener Class Reference

Inherits asyncore::dispatcher.

Collaboration diagram for rpki.https.http_listener:

Public Member Functions

- def __init__
- def handle_accept
- def handle_error

Public Attributes

- cert
- dynamic_ta
- handlers
- key
- ta

Static Public Attributes

- log = log_method

14.105.1 Detailed Description

```
Listener for incoming HTTP(S) connections.
```

Definition at line 707 of file https.py.

14.105.2 Member Function Documentation

14.105.2.1 def rpki.https.http_listener.__init__ (*self*, *handlers*, *port* = `80`, *host* = `""`, *cert* = `None`, *key* = `None`, *ta* = `None`, *dynamic_ta* = `None`, *af* = supported_address_families`[0]`)

Definition at line 714 of file https.py.

14.105.2.2 def rpki.https.http_listener.handle_accept (*self*)

```
Asyncore says we have an incoming connection, spawn an http_server
stream for it and pass along all of our handler and TLS data.
```

Definition at line 735 of file https.py.

14.105.2.3 def rpki.https.http_listener.handle_error (*self*)

```
Asyncore signaled an error, pass it along or log it.
```

Definition at line 748 of file https.py.

14.105.3 Member Data Documentation

14.105.3.1 rpki.https.http_listener.cert

Definition at line 718 of file https.py.

14.105.3.2 rpki.https.http_listener.dynamic_ta

Definition at line 721 of file https.py.

14.105.3.3 rpki.https.http_listener.handlers

Definition at line 717 of file https.py.

14.105.3.4 rpki.https.http_listener.key

Definition at line 719 of file https.py.

14.105.3.5 rpki.https.http_listener.log = log_method [static]

Definition at line 712 of file https.py.

14.105.3.6 rpki.https.http_listener.ta

Definition at line 720 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

14.106 rpki.https.http_message Class Reference

Inherits object.

Inherited by rpki.https.http_request, and rpki.https.http_response.

Collaboration diagram for rpki.https.http_message:

Public Member Functions

- def __init__
- def __str__
- def format
- def normalize_headers
- def parse_from_wire
- def parse_version
- def persistent

Public Attributes

- body
- headers
- version

Static Public Attributes

- string software_name = "ISC RPKI library"

14.106.1 Detailed Description

```
Virtual class representing of one HTTP message.
```

Definition at line 90 of file https.py.

14.106.2 Member Function Documentation

14.106.2.1 def rpki.https.http_message.__init__ (*self*, *version* = `None`, *body* = `None`, *headers* = `None`)

Definition at line 97 of file https.py.

14.106.2.2 def rpki.https.http_message.__str__ (*self*)

Definition at line 155 of file https.py.

14.106.2.3 def rpki.https.http_message.format (*self*)

```
Format an outgoing HTTP message.
```

Definition at line 140 of file https.py.

14.106.2.4 def rpki.https.http_message.normalize_headers (*self*, *headers* = None)

```
Clean up (some of) the horrible messes that HTTP allows in its
headers.
```

Definition at line 103 of file https.py.

14.106.2.5 def rpki.https.http_message.parse_from_wire (*cls*, *headers*)

```
Parse and normalize an incoming HTTP message.
```

Definition at line 126 of file https.py.

14.106.2.6 def rpki.https.http_message.parse_version (*self*, *version*)

```
Parse HTTP version, raise an exception if we can't.
```

Definition at line 158 of file https.py.

14.106.2.7 def rpki.https.http_message.persistent (*self*)

```
Figure out whether this HTTP message encourages a persistent connection.
```

Definition at line 166 of file https.py.

14.106.3 Member Data Documentation

14.106.3.1 rpki.https.http_message.body

Definition at line 99 of file https.py.

14.106.3.2 rpki.https.http_message.headers

Definition at line 100 of file https.py.

14.106.3.3 string rpki.https.http_message.software_name = "ISC RPKI library" [static]

Definition at line 95 of file https.py.

14.106.3.4 rpki.https.http_message.version

Definition at line 98 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

14.107 rpki.https.http_queue Class Reference

Inherits object.

Collaboration diagram for rpki.https.http_queue:

Public Member Functions

- def __init__
- def detach
- def request
- def restart
- def return_result
- def send_request

Public Attributes

- cert
- client
- hostport
- key
- queue
- ta

Static Public Attributes

- log = log_method

14.107.1 Detailed Description

```
Queue of pending HTTP requests for a single destination.  This class
is very tightly coupled to http_client; http_client handles the HTTP
stream itself, this class provides a slightly higher-level API.
```

Definition at line 929 of file https.py.

14.107.2 Member Function Documentation

14.107.2.1 def rpki.https.http_queue.__init__ (*self*, *hostport*, *cert* = `None`, *key* = `None`, *ta* = `()`)

Definition at line 938 of file https.py.

14.107.2.2 def rpki.https.http_queue.detach (*self*, *client_*)

```
Detatch a client from this queue.  Silently ignores attempting to
detach a client that is not attached to this queue, to simplify
handling of what otherwise would be a nasty set of race
conditions.
```

Definition at line 986 of file https.py.

14.107.2.3 def rpki.https.http_queue.request (*self*, *requests*)

```
Append http_request object(s) to this queue.
```

Definition at line 948 of file https.py.

14.107.2.4 def rpki.https.http_queue.restart (*self*)

```
Send next request for this queue, if we can.  This may involve
starting a new http_client stream, reusing an existing idle
stream, or just ignoring this request if there's an active client
stream already; in the last case, handling of the response (or
exception, or timeout) for the query currently in progress will
call this method when it's time to kick out the next query.
```

Definition at line 955 of file https.py.

14.107.2.5 def rpki.https.http_queue.return_result (*self*, *result*)

```
Client stream has returned a result, which we need to pass along
to the original caller.  Result may be either an HTTP response
message or an exception.  In either case, once we're done
processing this result, kick off next message in the queue, if any.
```

Definition at line 997 of file https.py.

14.107.2.6 def rpki.https.http_queue.send_request (*self*)

```
Kick out the next query in this queue, if any.
```

Definition at line 979 of file https.py.

14.107.3 Member Data Documentation

14.107.3.1 rpki.https.http_queue.cert

Definition at line 944 of file https.py.

14.107.3.2 rpki.https.http_queue.client

Definition at line 942 of file https.py.

14.107.3.3 rpki.https.http_queue.hostport

Definition at line 941 of file https.py.

14.107.3.4 rpki.https.http_queue.key

Definition at line 945 of file https.py.

14.107.3.5 rpki.https.http_queue.log = log_method [static]

Definition at line 936 of file https.py.

14.107.3.6 rpki.https.http_queue.queue

Definition at line 943 of file https.py.

14.107.3.7 rpki.https.http_queue.ta

Definition at line 946 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

14.108 rpki.https.http_request Class Reference

Inherits rpki::https::http_message.

Collaboration diagram for rpki.https.http_request:

Public Member Functions

- def __init__
- def format_first_line
- def parse_first_line

Public Attributes

- callback
- cmd
- errback
- path
- retried

14.108.1 Detailed Description

```
HTTP request message.
```

Definition at line 178 of file https.py.

14.108.2 Member Function Documentation

14.108.2.1 def rpki.https.http_request.__init__ (*self*, *cmd* = `None`, *path* = `None`, *version* = default_http_version, *body* = `None`, *callback* = `None`, *errback* = `None`, *headers*)

Definition at line 183 of file https.py.

14.108.2.2 def rpki.https.http_request.format_first_line (*self*)

```
Format first line of HTTP request message, and set up the
User-Agent header.
```

Definition at line 200 of file https.py.

14.108.2.3 def rpki.https.http_request.parse_first_line (*self*, *cmd*, *path*, *version*)

```
Parse first line of HTTP request message.
```

Definition at line 192 of file https.py.

14.108.3 Member Data Documentation

14.108.3.1 rpki.https.http_request.callback

Definition at line 188 of file https.py.

14.108.3.2 rpki.https.http_request.cmd

Definition at line 186 of file https.py.

14.108.3.3 rpki.https.http_request.errback

Definition at line 189 of file https.py.

14.108.3.4 rpki.https.http_request.path

Definition at line 187 of file https.py.

14.108.3.5 rpki.https.http_request.retried

Definition at line 190 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

14.109 rpki.https.http_response Class Reference

Inherits rpki::https::http_message.

Collaboration diagram for rpki.https.http_response:

Public Member Functions

- def __init__
- def format_first_line
- def parse_first_line

Public Attributes

- code
- reason

14.109.1 Detailed Description

```
HTTP response message.
```

Definition at line 208 of file https.py.

14.109.2 Member Function Documentation

14.109.2.1 def rpki.https.http_response.__init__ (*self*, *code* = `None`, *reason* = `None`, *version* = default_http_version, *body* = `None`, *headers*)

Definition at line 213 of file https.py.

14.109.2.2 def rpki.https.http_response.format_first_line (*self*)

```
Format first line of HTTP response message, and set up Date and
Server headers.
```

Definition at line 226 of file https.py.

14.109.2.3 def rpki.https.http_response.parse_first_line (*self*, *version*, *code*, *reason*)

```
Parse first line of HTTP response message.
```

Definition at line 218 of file https.py.

14.109.3 Member Data Documentation

14.109.3.1 rpki.https.http_response.code

Definition at line 215 of file https.py.

14.109.3.2 rpki.https.http_response.reason

Definition at line 216 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

14.110 rpki.https.http_server Class Reference

Inherits rpki::https::http_stream.

Collaboration diagram for rpki.https.http_server:

Public Member Functions

- def __init__
- def find_handler
- def handle_message
- def handle_no_content_length
- def send_error

- def send_message
- def send_reply
- def tls_accept

Public Attributes

- expect_close
- handlers
- retry_read
- retry_write
- tls

Static Public Attributes

- parse_type = http_request

  Stream parser should look for incoming HTTP request messages.

- timeout = default_server_timeout

  Use the default server timeout value set in the module header.

14.110.1 Detailed Description

```
HTTP(S) server stream.
```

Definition at line 561 of file https.py.

14.110.2 Member Function Documentation

14.110.2.1 def rpki.https.http_server.__init__ (*self*, *sock*, *handlers*, *cert* = `None`, *key* = `None`, *ta* = `()`, *dynamic_ta* = `None`)

Definition at line 574 of file https.py.

14.110.2.2 def rpki.https.http_server.find_handler (*self*, *path*)

```
Helper method to search self.handlers.
```

Definition at line 635 of file https.py.

14.110.2.3 def rpki.https.http_server.handle_message (*self*)

```
TLS and HTTP layers managed to deliver a complete HTTP request to
us, figure out what to do with it.  Check the command and
Content-Type, look for a handler, and if everything looks right,
pass the message body, path, and a reply callback to the handler.
```

Definition at line 644 of file https.py.

14.110.2.4 def rpki.https.http_server.handle_no_content_length (*self*)

```
Handle an incoming message that used neither chunking nor a
Content-Length header (that is: this message will be the last one
in this server stream).  No special action required.
```

Definition at line 627 of file https.py.

14.110.2.5 def rpki.https.http_server.send_error (*self*, *code*, *reason*)

```
Send an error response to this request.
```

Definition at line 673 of file https.py.

14.110.2.6 def rpki.https.http_server.send_message (*self*, *code*, *reason* = "OK", *body* = None)

```
Queue up reply message.  If both parties agree that connection is
persistant, and if no error occurred, restart this stream to
listen for next message; otherwise, queue up a close event for
this stream so it will shut down once the reply has been sent.
```

Definition at line 685 of file https.py.

14.110.2.7 def rpki.https.http_server.send_reply (*self*, *code*, *body*)

```
Send a reply to this request.
```

Definition at line 679 of file https.py.

14.110.2.8 def rpki.https.http_server.tls_accept (*self*)

```
Set up TLS for server side connection, handling all the whacky
OpenSSL exceptions from TLS.

SSLErrorSSLError exceptions are particularly nasty, because all
too often they indicate a certificate lookup failure deep within
the guts of OpenSSL's TLS connection setup logic.  Extracting
anything resembling a Python data structure from a handler called
that deep inside the OpenSSL TLS library, while theoretically
possible, runs a high risk of triggering some kind of memory leak
or corruption.  So, for now, we just get back a long text string,
which we break up and log but don't attempt to process further.
```

Definition at line 596 of file https.py.

14.110.3 Member Data Documentation

14.110.3.1 rpki.https.http_server.expect_close

Definition at line 578 of file https.py.

14.110.3.2 rpki.https.http_server.handlers

Definition at line 576 of file https.py.

14.110.3.3 rpki::https.http_server::parse_type = http_request [static]

Stream parser should look for incoming HTTP request messages.

Definition at line 568 of file https.py.

14.110.3.4 rpki.https.http_server.retry_read

Reimplemented from rpki.https.http_stream.

Definition at line 613 of file https.py.

14.110.3.5 rpki.https.http_server.retry_write

Reimplemented from rpki.https.http_stream.

Definition at line 615 of file https.py.

14.110.3.6 rpki::https.http_server::timeout = default_server_timeout [static]

Use the default server timeout value set in the module header.

Definition at line 572 of file https.py.

14.110.3.7 rpki.https.http_server.tls

Reimplemented from rpki.https.http_stream.

Definition at line 582 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

14.111 rpki.https.http_stream Class Reference

Inherits asynchat::async_chat.

Inherited by rpki.https.http_client, and rpki.https.http_server.

Collaboration diagram for rpki.https.http_stream:

Public Member Functions

- def __init__
- def chunk_body
- def chunk_discard_crlf
- def chunk_discard_trailer
- def chunk_header

- def close
- def collect_incoming_data
- def found_terminator
- def get_buffer
- def handle_body
- def handle_close
- def handle_error
- def handle_read
- def handle_timeout
- def handle_write
- def initiate_send
- def log_cert
- def readable
- def recv
- def restart
- def send
- def update_timeout
- def writeable

Public Attributes

- buffer
- chunk_handler
- msg
- timer

Static Public Attributes

- log = log_method
- retry_read = None
- retry_write = None
- tls = None

14.111.1 Detailed Description

```
Virtual class representing an HTTP message stream.
```

Definition at line 243 of file https.py.

14.111.2 Member Function Documentation

14.111.2.1 def rpki.https.http_stream.__init__ (*self*, *sock* = None)

Definition at line 253 of file https.py.

14.111.2.2 def rpki.https.http_stream.chunk_body (*self*)

```
Asynchat just handed us what should be the body of a chunk of the
body of a chunked message (sic).  Save it, and prepare to move on
to the next chunk.
```

Definition at line 343 of file https.py.

14.111.2.3 def rpki.https.http_stream.chunk_discard_crlf (*self*)

```
Consume the CRLF that terminates a chunk, reinitialize chunk
decoder to be ready for the next chunk.
```

Definition at line 355 of file https.py.

14.111.2.4 def rpki.https.http_stream.chunk_discard_trailer (*self*)

```
Consume chunk trailer, which should be empty, then (finally!) exit
the chunk decoder and hand complete message off to the application.
```

Definition at line 365 of file https.py.

14.111.2.5 def rpki.https.http_stream.chunk_header (*self*)

```
Asynchat just handed us what should be the header of one chunk of
a chunked encoding stream.  If this chunk has a body, set the
stream up to read it; otherwise, this is the last chunk, so start
the process of exiting the chunk decoder.
```

Definition at line 327 of file https.py.

14.111.2.6 def rpki.https.http_stream.close (*self*, *force* = `False`)

```
Close the stream.

Graceful shutdown of a TLS connection requires multiple calls to
the underlying TLS code.  If the connection should be closed right
now without waiting (perhaps because it's already dead and we're
just cleaning up), call with force = True.
```

Definition at line 521 of file https.py.

14.111.2.7 def rpki.https.http_stream.collect_incoming_data (*self*, *data*)

```
Buffer incoming data from asynchat.
```

Definition at line 279 of file https.py.

14.111.2.8 def rpki.https.http_stream.found_terminator (*self*)

```
Asynchat reported that it found whatever terminator we set, so
figure out what to do next.  This can be messy, because we can be
in any of several different states:

@li We might be handling chunked HTTP, in which case we have to
initialize the chunk decoder;

@li We might have found the end of the message body, in which case
we can (finally) process it; or

@li We might have just gotten to the end of the message headers,
in which case we have to parse them to figure out which of three
separate mechanisms (chunked, content-length, TCP close) is going
to tell us how to find the end of the message body.
```

Definition at line 294 of file https.py.

14.111.2.9 def rpki.https.http_stream.get_buffer (*self*)

```
Consume data buffered from asynchat.
```

Definition at line 286 of file https.py.

14.111.2.10 def rpki.https.http_stream.handle_body (*self*)

```
Hand normal (not chunked) message off to the application.
```

Definition at line 376 of file https.py.

14.111.2.11 def rpki.https.http_stream.handle_close (*self*)

```
Wrapper around asynchat connection close handler, so that we can
log the event.
```

Reimplemented in rpki.https.http_client.

Definition at line 406 of file https.py.

14.111.2.12 def rpki.https.http_stream.handle_error (*self*)

```
Asynchat (or asyncore, or somebody) raised an exception.  See
whether it's one we should just pass along, otherwise log a stack
trace and close the stream.
```

Reimplemented in rpki.https.http_client.

Definition at line 383 of file https.py.

14.111.2.13 def rpki.https.http_stream.handle_read (*self*)

```
Asyncore says socket is readable.  Make sure there's no TLS write
already in progress, retry previous read operation if we had one
that was waiting for more input, otherwise try to read some data,
and handle all the weird OpenSSL exceptions that the TLS code
throws.
```

Definition at line 450 of file https.py.

14.111.2.14 def rpki.https.http_stream.handle_timeout (*self*)

```
Inactivity timer expired, close connection with prejudice.
```

Reimplemented in rpki.https.http_client.

Definition at line 399 of file https.py.

14.111.2.15 def rpki.https.http_stream.handle_write (*self*)

```
Asyncore says socket is writeable.  Make sure there's no TLS read
already in progress, retry previous write operation if we had one
that was blocked on the socket, otherwise try to write some data.
Handling all the weird OpenSSL exceptions that TLS throws is our
caller's problem.
```

Definition at line 478 of file https.py.

14.111.2.16 def rpki.https.http_stream.initiate_send (*self*)

```
Initiate a write operation.  This is just a wrapper around the
asynchat method, to handle all the whacky TLS exceptions.
```

Definition at line 502 of file https.py.

14.111.2.17 def rpki.https.http_stream.log_cert (*self*, *tag*, *x*)

```
Log HTTPS certificates, if certificate debugging is enabled.
```

Definition at line 554 of file https.py.

14.111.2.18 def rpki.https.http_stream.readable (*self*)

```
TLS replacement for normal asynchat .readable() method.  A TLS
connection that's blocked waiting for TLS write is considered not
readable even if the underlying socket is.
```

Definition at line 434 of file https.py.

14.111.2.19 def rpki.https.http_stream.recv (*self*, *buffer_size*)

```
TLS replacement for normal asyncore .recv() method.  Throw an
exception if TLS hasn't been started or if TLS I/O was already in
progress, otherwise hand off to the TLS code.
```

Definition at line 424 of file https.py.

14.111.2.20 def rpki.https.http_stream.restart (*self*)

```
(Re)start HTTP message parser, reset timer.
```

Definition at line 259 of file https.py.

14.111.2.21 def rpki.https.http_stream.send (*self*, *data*)

```
TLS replacement for normal asyncore .send() method.  Throw an
exception if TLS hasn't been started or if TLS I/O was already in
progress, otherwise hand off to the TLS code.
```

Definition at line 414 of file https.py.

14.111.2.22 def rpki.https.http_stream.update_timeout (*self*)

```
Put this stream's timer in known good state: set it to the
stream's timeout value if we're doing timeouts, otherwise clear
it.
```

Definition at line 268 of file https.py.

14.111.2.23 def rpki.https.http_stream.writeable (*self*)

```
TLS replacement for normal asynchat .writeable() method.  A TLS
connection that's blocked waiting for TLS read is considered not
writeable even if the underlying socket is.
```

Definition at line 442 of file https.py.

14.111.3 Member Data Documentation

14.111.3.1 rpki.https.http_stream.buffer

Definition at line 255 of file https.py.

14.111.3.2 rpki.https.http_stream.chunk_handler

Definition at line 264 of file https.py.

14.111.3.3 rpki.https.http_stream.log = log_method [static]

Definition at line 248 of file https.py.

14.111.3.4 rpki.https.http_stream.msg

Definition at line 317 of file https.py.

14.111.3.5 rpki.https.http_stream.retry_read = None [static]

Reimplemented in rpki.https.http_server, and rpki.https.http_client.

Definition at line 250 of file https.py.

14.111.3.6 rpki.https.http_stream.retry_write = None [static]

Reimplemented in rpki.https.http_server, and rpki.https.http_client.

Definition at line 251 of file https.py.

14.111.3.7 rpki.https.http_stream.timer

Definition at line 256 of file https.py.

14.111.3.8 rpki.https.http_stream.tls = None [static]

Reimplemented in rpki.https.http_server, and rpki.https.http_client.

Definition at line 249 of file https.py.

The documentation for this class was generated from the following file:

- https.py (3191)

14.112 rpki.ipaddrs.v4addr Class Reference

Inherits long.

Collaboration diagram for rpki.ipaddrs.v4addr:

Public Member Functions

- def __new__
- def __str__
- def from_bytes
- def to_bytes

Static Public Attributes

- int bits = 32

14.112.1 Detailed Description

```
IPv4 address.

Derived from long, but supports IPv4 print syntax.
```

Definition at line 47 of file ipaddrs.py.

14.112.2 Member Function Documentation

14.112.2.1 def rpki.ipaddrs.v4addr.__new__ (*cls*, *x*)

```
Construct a v4addr object.
```

Definition at line 56 of file ipaddrs.py.

14.112.2.2 def rpki.ipaddrs.v4addr.__str__ (*self*)

```
Convert a v4addr object to string format.
```

Definition at line 74 of file ipaddrs.py.

14.112.2.3 def rpki.ipaddrs.v4addr.from_bytes (*cls*, *x*)

```
Convert from a raw byte string to a v4addr object.
```

Definition at line 70 of file ipaddrs.py.

14.112.2.4 def rpki.ipaddrs.v4addr.to_bytes (*self*)

```
Convert a v4addr object to a raw byte string.
```

Definition at line 65 of file ipaddrs.py.

14.112.3 Member Data Documentation

14.112.3.1 int rpki.ipaddrs.v4addr.bits = 32 [static]

Definition at line 54 of file ipaddrs.py.

The documentation for this class was generated from the following file:

- ipaddrs.py (2424)

14.113 rpki.ipaddrs.v6addr Class Reference

Inherits long.

Collaboration diagram for rpki.ipaddrs.v6addr:

Public Member Functions

- def __new__
- def __str__
- def from_bytes
- def to_bytes

Static Public Attributes

- int bits = 128

14.113.1 Detailed Description

```
IPv6 address.

Derived from long, but supports IPv6 print syntax.
```

Definition at line 78 of file ipaddrs.py.

14.113.2 Member Function Documentation

14.113.2.1 def rpki.ipaddrs.v6addr.__new__ (*cls*, *x*)

```
Construct a v6addr object.
```

Definition at line 87 of file ipaddrs.py.

14.113.2.2 def rpki.ipaddrs.v6addr.__str__ (*self*)

```
Convert a v6addr object to string format.
```

Definition at line 104 of file ipaddrs.py.

14.113.2.3 def rpki.ipaddrs.v6addr.from_bytes (*cls*, *x*)

```
Convert from a raw byte string to a v6addr object.
```

Definition at line 99 of file ipaddrs.py.

14.113.2.4 def rpki.ipaddrs.v6addr.to_bytes (*self*)

```
Convert a v6addr object to a raw byte string.
```

Definition at line 94 of file ipaddrs.py.

14.113.3 Member Data Documentation

14.113.3.1 int rpki.ipaddrs.v6addr.bits = 128 [static]

Definition at line 85 of file ipaddrs.py.

The documentation for this class was generated from the following file:

- ipaddrs.py (2424)

14.114 rpki.left_right.bsc_elt Class Reference

Inherits rpki::left_right::data_elt.

Inherited by irbe_cli.bsc_elt.

Collaboration diagram for rpki.left_right.bsc_elt:

Public Member Functions

- def children
- def parents
- def repositories
- def serve_pre_save_hook

Static Public Attributes

- tuple attributes = ("action", "tag", "self_handle", "bsc_handle", "key_type", "hash_alg", "key_length")

  XML attributes for this element.

- tuple booleans = ("generate_keypair",)

  Boolean attributes (value "yes" or "no") for this element.

- string element_name = "bsc"
- tuple elements = ("signing_cert", "signing_cert_crl", "pkcs10_request")

  XML elements contained by this element.

- tuple handles = (("self", self_elt),)
- pkcs10_request = None
- private_key_id = None
- signing_cert = None
- signing_cert_crl = None
- tuple sql_template

14.114.1 Detailed Description

```
<bsc/> (Business Signing Context) element.
```

Definition at line 526 of file left_right.py.

14.114.2 Member Function Documentation

14.114.2.1 def rpki.left_right.bsc_elt.children (*self*)

```
Fetch all child objects that link to this BSC object.
```

Definition at line 557 of file left_right.py.

14.114.2.2 def rpki.left_right.bsc_elt.parents (*self*)

```
Fetch all parent objects that link to this BSC object.
```

Definition at line 553 of file left_right.py.

14.114.2.3 def rpki.left_right.bsc_elt.repositories (*self*)

```
Fetch all repository objects that link to this BSC object.
```

Definition at line 549 of file left_right.py.

14.114.2.4 def rpki.left_right.bsc_elt.serve_pre_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Extra server actions for bsc_elt -- handle key generation.  For
now this only allows RSA with SHA-256.
```

Reimplemented from rpki.left_right.data_elt.

Definition at line 561 of file left_right.py.

14.114.3 Member Data Documentation

14.114.3.1 tuple rpki.left_right.bsc_elt.attributes = ("action", "tag", "self_handle", "bsc_handle", "key_type", "hash_alg", "key_length") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 532 of file left_right.py.

14.114.3.2 tuple rpki.left_right.bsc_elt.booleans = ("generate_keypair",) [static]

Boolean attributes (value "yes" or "no") for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 534 of file left_right.py.

14.114.3.3 string rpki.left_right.bsc_elt.element_name = "bsc" [static]

Definition at line 531 of file left_right.py.

14.114.3.4 tuple rpki.left_right.bsc_elt.elements = ("signing_cert", "signing_cert_crl", "pkcs10_request") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 533 of file left_right.py.

14.114.3.5 tuple rpki.left_right.bsc_elt.handles = (("self", self_elt),) [static]

Reimplemented from rpki.left_right.data_elt.

Definition at line 542 of file left_right.py.

14.114.3.6 rpki.left_right.bsc_elt.pkcs10_request = None [static]

Definition at line 545 of file left_right.py.

14.114.3.7 rpki.left_right.bsc_elt.private_key_id = None [static]

Definition at line 544 of file left_right.py.

14.114.3.8 rpki.left_right.bsc_elt.signing_cert = None [static]

Reimplemented in irbe_cli.bsc_elt.

Definition at line 546 of file left_right.py.

14.114.3.9 rpki.left_right.bsc_elt.signing_cert_crl = None [static]

Reimplemented in irbe_cli.bsc_elt.

Definition at line 547 of file left_right.py.

14.114.3.10 tuple rpki.left_right.bsc_elt.sql_template [static]

Initial value:

```
rpki.sql.template("bsc", "bsc_id", "bsc_handle",
                                   "self_id", "hash_alg",
                                   ("private_key_id", rpki.x509.RSA),
                                   ("pkcs10_request", rpki.x509.PKCS10),
                                   ("signing_cert", rpki.x509.X509),
                                   ("signing_cert_crl", rpki.x509.CRL))
```

Definition at line 536 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

14.115 rpki.left_right.child_elt Class Reference

Inherits rpki::left_right::data_elt.

Inherited by irbe_cli.child_elt.

Collaboration diagram for rpki.left_right.child_elt:

Public Member Functions

- def ca_from_class_name
- def child_certs
- def endElement
- def parents
- def serve_destroy_hook
- def serve_post_save_hook
- def serve_up_down

Static Public Attributes

- tuple attributes = ("action", "tag", "self_handle", "child_handle", "bsc_-handle")

  XML attributes for this element.

- tuple booleans = ("reissue",)

  Boolean attributes (value "yes" or "no") for this element.

- bpki_cert = None
- bpki_glue = None
- clear_https_ta_cache = False
- string element_name = "child"
- tuple elements = ("bpki_cert", "bpki_glue")

  XML elements contained by this element.

- tuple handles = (("self", self_elt), ("bsc", bsc_elt))
- tuple sql_template

14.115.1 Detailed Description

```
<child/> element.
```

Definition at line 805 of file left_right.py.

14.115.2 Member Function Documentation

14.115.2.1 def rpki.left_right.child_elt.ca_from_class_name (*self*, *class_name*)

```
Fetch the CA corresponding to an up-down class_name.
```

Definition at line 834 of file left_right.py.

14.115.2.2 def rpki.left_right.child_elt.child_certs (*self*, *ca_detail* = `None`, *ski* = `None`, *unique* = `False`)

```
Fetch all child_cert objects that link to this child object.
```

Definition at line 826 of file left_right.py.

14.115.2.3 def rpki.left_right.child_elt.endElement (*self*, *stack*, *name*, *text*)

```
Handle subelements of <child/> element.  These require special
handling because modifying them invalidates the HTTPS trust anchor
cache.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 866 of file left_right.py.

14.115.2.4 def rpki.left_right.child_elt.parents (*self*)

```
Fetch all parent objects that link to self object to which this child object links.
```

Definition at line 830 of file left_right.py.

14.115.2.5 def rpki.left_right.child_elt.serve_destroy_hook (*self*, *cb*, *eb*)

```
Extra server actions when destroying a child_elt.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 858 of file left_right.py.

14.115.2.6 def rpki.left_right.child_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Extra server actions for child_elt.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 848 of file left_right.py.

14.115.2.7 def rpki.left_right.child_elt.serve_up_down (*self*, *query*, *callback*)

```
Outer layer of server handling for one up-down PDU from this child.
```

Definition at line 876 of file left_right.py.

14.115.3 Member Data Documentation

14.115.3.1 tuple rpki.left_right.child_elt.attributes = ("action", "tag", "self_handle", "child_handle", "bsc_handle") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 811 of file left_right.py.

14.115.3.2 tuple rpki.left_right.child_elt.booleans = ("reissue",) [static]

Boolean attributes (value "yes" or "no") for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 813 of file left_right.py.

14.115.3.3 rpki.left_right.child_elt.bpki_cert = None [static]

Definition at line 822 of file left_right.py.

14.115.3.4 rpki.left_right.child_elt.bpki_glue = None [static]

Definition at line 823 of file left_right.py.

14.115.3.5 rpki.left_right.child_elt.clear_https_ta_cache = False [static]

Definition at line 824 of file left_right.py.

14.115.3.6 string rpki.left_right.child_elt.element_name = "child" [static]

Definition at line 810 of file left_right.py.

14.115.3.7 tuple rpki.left_right.child_elt.elements = ("bpki_cert", "bpki_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 812 of file left_right.py.

14.115.3.8 tuple rpki.left_right.child_elt.handles = (("self", self_elt), ("bsc", bsc_elt)) [static]

Reimplemented from rpki.left_right.data_elt.

Definition at line 820 of file left_right.py.

14.115.3.9 tuple rpki.left_right.child_elt.sql_template [static]

Initial value:

```
rpki.sql.template("child", "child_id", "child_handle",
                                  "self_id", "bsc_id",
                                  ("bpki_cert", rpki.x509.X509),
                                  ("bpki_glue", rpki.x509.X509))
```

Definition at line 815 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

14.116 rpki.left_right.cms_msg Class Reference

Inherits rpki::x509::XML_CMS_object.

Inherited by irbe_cli.left_right_cms_msg.

Collaboration diagram for rpki.left_right.cms_msg:

Static Public Attributes

- string encoding = "us-ascii"
- saxify = sax_handler.saxify
- schema = rpki.relaxng.left_right

14.116.1 Detailed Description

```
Class to hold a CMS-signed left-right PDU.
```

Definition at line 1120 of file left_right.py.

14.116.2 Member Data Documentation

14.116.2.1 string rpki.left_right.cms_msg.encoding = "us-ascii" [static]

Definition at line 1125 of file left_right.py.

14.116.2.2 rpki.left_right.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented in irbe_cli.left_right_cms_msg.

Definition at line 1127 of file left_right.py.

14.116.2.3 rpki.left_right.cms_msg.schema = rpki.relaxng.left_right [static]

Definition at line 1126 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

14.117 rpki.left_right.data_elt Class Reference

Inherits rpki::xml_utils::data_elt, rpki::sql::sql_persistent, and rpki::left_right::left_-right_namespace.

Inherited by rpki.left_right.bsc_elt, rpki.left_right.child_elt, rpki.left_right.parent_elt, rpki.left_right.repository_elt, and rpki.left_right.self_elt.

Collaboration diagram for rpki.left_right.data_elt:

Public Member Functions

- def bsc
- def make_reply_clone_hook
- def self
- def serve_fetch_all
- def serve_fetch_handle
- def serve_fetch_one_maybe
- def serve_pre_save_hook

Static Public Attributes

- tuple handles = ()
- self_handle = None
- self_id = None

14.117.1 Detailed Description

```
Virtual class for top-level left-right protocol data elements.
```

Definition at line 50 of file left_right.py.

14.117.2 Member Function Documentation

14.117.2.1 def rpki.left_right.data_elt.bsc (*self*)

```
Return BSC object to which this object links.
```

Definition at line 64 of file left_right.py.

14.117.2.2 def rpki.left_right.data_elt.make_reply_clone_hook (*self*, *r_pdu*)

```
Set handles when cloning, including _id -> _handle translation.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 68 of file left_right.py.

14.117.2.3 def rpki.left_right.data_elt.self (*self*)

```
Fetch self object to which this object links.
```

Definition at line 60 of file left_right.py.

14.117.2.4 def rpki.left_right.data_elt.serve_fetch_all (*self*)

```
Find the objects on which a list method should operate.
```

Reimplemented in rpki.left_right.self_elt.

Definition at line 99 of file left_right.py.

14.117.2.5 def rpki.left_right.data_elt.serve_fetch_handle (*cls*, *gctx*, *self_id*, *handle*)

```
Find an object based on its handle.
```

Reimplemented in rpki.left_right.self_elt.

Definition at line 84 of file left_right.py.

14.117.2.6 def rpki.left_right.data_elt.serve_fetch_one_maybe (*self*)

```
Find the object on which a get, set, or destroy method should
operate, or which would conflict with a create method.
```

Reimplemented in rpki.left_right.self_elt.

Definition at line 90 of file left_right.py.

14.117.2.7 def rpki.left_right.data_elt.serve_pre_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Hook to do _handle => _id translation before saving.

self is always the object to be saved to SQL.  For create
operations, self and q_pdu are be the same object; for set
operations, self is the pre-existing object from SQL and q_pdu is
the set request received from the the IRBE.
```

Reimplemented from rpki.xml_utils.data_elt.

Reimplemented in rpki.left_right.bsc_elt.

Definition at line 106 of file left_right.py.

14.117.3 Member Data Documentation

14.117.3.1 tuple rpki.left_right.data_elt.handles = () [static]

Reimplemented in rpki.left_right.self_elt, rpki.left_right.bsc_elt, rpki.left_right.repository_elt, rpki.left_right.parent_elt, and rpki.left_right.child_elt.

Definition at line 55 of file left_right.py.

14.117.3.2 rpki.left_right.data_elt.self_handle = None [static]

Definition at line 58 of file left_right.py.

14.117.3.3 rpki.left_right.data_elt.self_id = None [static]

Definition at line 57 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

14.118 rpki.left_right.left_right_namespace Class Reference

Inherits object.

Inherited by rpki.left_right.data_elt, rpki.left_right.list_published_objects_elt, rpki.left_right.list_received_resources_elt, rpki.left_right.list_resources_elt, rpki.left_right.list_roa_requests_elt, rpki.left_right.msg, and rpki.left_right.report_error_elt.

Collaboration diagram for rpki.left_right.left_right_namespace:

Static Public Attributes

- dictionary nsmap = { None : xmlns }
- string xmlns = "http://www.hactrn.net/uris/rpki/left-right-spec/"

14.118.1 Detailed Description

```
XML namespace parameters for left-right protocol.
```

Definition at line 42 of file left_right.py.

14.118.2 Member Data Documentation

14.118.2.1 dictionary rpki.left_right.left_right_namespace.nsmap = { None : xmlns } [static]

Definition at line 48 of file left_right.py.

14.118.2.2 string rpki.left_right.left_right_namespace.xmlns = "http://www.hactrn.net/uris/rpki/left-right-spec/" [static]

Definition at line 47 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

14.119 rpki.left_right.list_published_objects_elt Class Reference

Inherits rpki::xml_utils::text_elt, and rpki::left_right::left_right_namespace.

Inherited by irbe_cli.list_published_objects_elt.

Collaboration diagram for rpki.left_right.list_published_objects_elt:

Public Member Functions

- def make_reply
- def serve_dispatch

Static Public Attributes

- tuple attributes = ("self_handle", "tag", "uri")

  XML attributes for this element.

- string element_name = "list_published_objects"
- obj = None
- string text_attribute = "obj"

  Name of the class attribute that holds the text value.

14.119.1 Detailed Description

```
<list_published_objects/> element.
```

Definition at line 968 of file left_right.py.

14.119.2 Member Function Documentation

14.119.2.1 def rpki.left_right.list_published_objects_elt.make_reply (*self*, *uri*, *obj*)

```
Generate one reply PDU.
```

Definition at line 995 of file left_right.py.

14.119.2.2 def rpki.left_right.list_published_objects_elt.serve_dispatch (*self*, *r_msg*, *cb*, *eb*)

```
Handle a <list_published_objects/> query.  The method name is a
misnomer here, there's no action attribute and no dispatch, we
just dump every published object for the specified <self/> and return.
```

Definition at line 979 of file left_right.py.

14.119.3 Member Data Documentation

14.119.3.1 tuple rpki.left_right.list_published_objects_elt.attributes = ("self_handle", "tag", "uri") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 974 of file left_right.py.

14.119.3.2 string rpki.left_right.list_published_objects_elt.element_name = "list_published_objects" [static]

Definition at line 973 of file left_right.py.

14.119.3.3 rpki.left_right.list_published_objects_elt.obj = None [static]

Definition at line 977 of file left_right.py.

14.119.3.4 string rpki.left_right.list_published_objects_elt.text_attribute = "obj" [static]

Name of the class attribute that holds the text value.

Reimplemented from rpki.xml_utils.text_elt.

Definition at line 975 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

14.120 rpki.left_right.list_received_resources_elt Class Reference

Inherits rpki::xml_utils::base_elt, and rpki::left_right::left_right_namespace.

Inherited by irbe_cli.list_received_resources_elt.

Collaboration diagram for rpki.left_right.list_received_resources_elt:

Public Member Functions

- def make_reply
- def serve_dispatch

Static Public Attributes

- tuple attributes

  XML attributes for this element.

- string element_name = "list_received_resources"

14.120.1 Detailed Description

```
<list_received_resources/> element.
```

Definition at line 1003 of file left_right.py.

14.120.2 Member Function Documentation

14.120.2.1 def rpki.left_right.list_received_resources_elt.make_reply (*self*, *uri*, *cert*)

```
Generate one reply PDU.
```

Definition at line 1026 of file left_right.py.

14.120.2.2 def rpki.left_right.list_received_resources_elt.serve_dispatch (*self*, *r_msg*, *cb*, *eb*)

```
Handle a <list_received_resources/> query.  The method name is a
misnomer here, there's no action attribute and no dispatch, we
just dump a bunch of data about every certificate issued to us by
one of our parents, then return.
```

Definition at line 1012 of file left_right.py.

14.120.3 Member Data Documentation

14.120.3.1 tuple rpki.left_right.list_received_resources_elt.attributes [static]

Initial value:

```
("self_handle", "tag",
                "notBefore", "notAfter", "uri", "sia_uri", "aia_uri", "asn", "ipv
      4", "ipv6")
```

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 1009 of file left_right.py.

14.120.3.2 string rpki.left_right.list_received_resources_elt.element_name = "list_received_resources" [static]

Definition at line 1008 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

14.121 rpki.left_right.list_resources_elt Class Reference

Inherits rpki::xml_utils::base_elt, and rpki::left_right::left_right_namespace.

Collaboration diagram for rpki.left_right.list_resources_elt:

Public Member Functions

- def startElement
- def toXML

Public Attributes

- asn

- ipv4
- ipv6

Static Public Attributes

- tuple attributes = ("self_handle", "tag", "child_handle", "valid_until", "asn", "ipv4", "ipv6")

  XML attributes for this element.

- string element_name = "list_resources"
- valid_until = None

14.121.1 Detailed Description

```
<list_resources/> element.
```

Definition at line 913 of file left_right.py.

14.121.2 Member Function Documentation

14.121.2.1 def rpki.left_right.list_resources_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle <list_resources/> element.  This requires special handling
due to the data types of some of the attributes.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 922 of file left_right.py.

14.121.2.2 def rpki.left_right.list_resources_elt.toXML (*self*)

```
Generate <list_resources/> element.  This requires special
handling due to the data types of some of the attributes.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 938 of file left_right.py.

14.121.3 Member Data Documentation

14.121.3.1 rpki.left_right.list_resources_elt.asn

Definition at line 932 of file left_right.py.

14.121.3.2 tuple rpki.left_right.list_resources_elt.attributes = ("self_handle", "tag", "child_handle", "valid_until", "asn", "ipv4", "ipv6") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 919 of file left_right.py.

14.121.3.3 string rpki.left_right.list_resources_elt.element_name = "list_resources" [static]

Definition at line 918 of file left_right.py.

14.121.3.4 rpki.left_right.list_resources_elt.ipv4

Definition at line 934 of file left_right.py.

14.121.3.5 rpki.left_right.list_resources_elt.ipv6

Definition at line 936 of file left_right.py.

14.121.3.6 rpki.left_right.list_resources_elt.valid_until = None [static]

Definition at line 920 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

14.122 rpki.left_right.list_roa_requests_elt Class Reference

Inherits rpki::xml_utils::base_elt, and rpki::left_right::left_right_namespace.

Collaboration diagram for rpki.left_right.list_roa_requests_elt:

Public Member Functions

- def startElement

Public Attributes

- ipv4
- ipv6

Static Public Attributes

- tuple attributes = ("self_handle", "tag", "asn", "ipv4", "ipv6")

  XML attributes for this element.

- string element_name = "list_roa_requests"

14.122.1 Detailed Description

```
<list_roa_requests/> element.
```

Definition at line 948 of file left_right.py.

14.122.2 Member Function Documentation

14.122.2.1 def rpki.left_right.list_roa_requests_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle <list_roa_requests/> element.  This requires special handling
due to the data types of some of the attributes.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 956 of file left_right.py.

14.122.3 Member Data Documentation

14.122.3.1 tuple rpki.left_right.list_roa_requests_elt.attributes = ("self_handle", "tag", "asn", "ipv4", "ipv6") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 954 of file left_right.py.

14.122.3.2 string rpki.left_right.list_roa_requests_elt.element_name = "list_roa_requests" [static]

Definition at line 953 of file left_right.py.

14.122.3.3 rpki.left_right.list_roa_requests_elt.ipv4

Definition at line 964 of file left_right.py.

14.122.3.4 rpki.left_right.list_roa_requests_elt.ipv6

Definition at line 966 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

14.123 rpki.left_right.msg Class Reference

Inherits rpki::xml_utils::msg, and rpki::left_right::left_right_namespace.

Inherited by irbe_cli.left_right_msg.

Collaboration diagram for rpki.left_right.msg:

Public Member Functions

- def serve_top_level

Static Public Attributes

- tuple pdus

Dispatch table of PDUs for this protocol.

- int version = 1

  Protocol version.

14.123.1 Detailed Description

```
Left-right PDU.
```

Definition at line 1066 of file left_right.py.

14.123.2 Member Function Documentation

14.123.2.1 def rpki.left_right.msg.serve_top_level (*self*, *gctx*, *cb*)

```
Serve one msg PDU.
```

Definition at line 1083 of file left_right.py.

14.123.3 Member Data Documentation

14.123.3.1 rpki::left_right.msg::pdus [static]

Initial value:

```
dict((x.element_name, x)
              for x in (self_elt, child_elt, parent_elt, bsc_elt, repository_elt,

                        list_resources_elt, list_roa_requests_elt,
                        list_published_objects_elt, list_received_resources_elt,
                        report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented in irbe_cli.left_right_msg.

Definition at line 1077 of file left_right.py.

14.123.3.2 rpki::left_right.msg::version = 1 [static]

Protocol version.

Reimplemented from rpki.xml_utils.msg.

Definition at line 1073 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

14.124 rpki.left_right.parent_elt Class Reference

Inherits rpki::left_right::data_elt.

Inherited by irbe_cli.parent_elt.

Collaboration diagram for rpki.left_right.parent_elt:

Public Member Functions

- def cas
- def query_up_down
- def repository
- def serve_post_save_hook
- def serve_rekey
- def serve_revoke
- def serve_revoke_forgotten

Static Public Attributes

- tuple attributes

  XML attributes for this element.

- tuple booleans = ("rekey", "reissue", "revoke", "revoke_forgotten")

  Boolean attributes (value "yes" or "no") for this element.

- bpki_cms_cert = None
- bpki_cms_glue = None
- bpki_https_cert = None
- bpki_https_glue = None
- string element_name = "parent"
- tuple elements = ("bpki_cms_cert", "bpki_cms_glue", "bpki_https_cert", "bpki_https_glue")

  XML elements contained by this element.

- tuple handles = (("self", self_elt), ("bsc", bsc_elt), ("repository", repository_elt))
- tuple sql_template

14.124.1 Detailed Description

```
<parent/> element.
```

Definition at line 656 of file left_right.py.

14.124.2 Member Function Documentation

14.124.2.1 def rpki.left_right.parent_elt.cas (*self*)

```
Fetch all CA objects that link to this parent object.
```

Definition at line 683 of file left_right.py.

14.124.2.2 def rpki.left_right.parent_elt.query_up_down (*self*, *q_pdu*, *cb*, *eb*)

```
Client code for sending one up-down query PDU to this parent.
```

Definition at line 759 of file left_right.py.

14.124.2.3 def rpki.left_right.parent_elt.repository (*self*)

```
Fetch repository object to which this parent object links.
```

Definition at line 679 of file left_right.py.

14.124.2.4 def rpki.left_right.parent_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Extra server actions for parent_elt.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 687 of file left_right.py.

14.124.2.5 def rpki.left_right.parent_elt.serve_rekey (*self*, *cb*, *eb*)

```
Handle a left-right rekey action for this parent.
```

Definition at line 703 of file left_right.py.

14.124.2.6 def rpki.left_right.parent_elt.serve_revoke (*self*, *cb*, *eb*)

```
Handle a left-right revoke action for this parent.
```

Definition at line 711 of file left_right.py.

14.124.2.7 def rpki.left_right.parent_elt.serve_revoke_forgotten (*self*, *cb*, *eb*)

```
Handle a left-right revoke_forgotten action for this parent.

This is a bit fiddly: we have to compare the result of an up-down
list query with what we have locally and identify the SKIs of any
certificates that have gone missing.  This should never happen in
ordinary operation, but can arise if we have somehow lost a
private key, in which case there is nothing more we can do with
the issued cert, so we have to clear it.  As this really is not
supposed to happen, we don't clear it automatically, instead we
require an explicit trigger.
```

Definition at line 719 of file left_right.py.

14.124.3 Member Data Documentation

14.124.3.1 tuple rpki.left_right.parent_elt.attributes [static]

Initial value:

```
("action", "tag", "self_handle", "parent_handle", "bsc_handle", "repository_handl
      e",
                "peer_contact_uri", "sia_base", "sender_name", "recipient_name")
```

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 662 of file left_right.py.

14.124.3.2 tuple rpki.left_right.parent_elt.booleans = ("rekey", "reissue", "revoke", "revoke_forgotten") [static]

Boolean attributes (value "yes" or "no") for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 665 of file left_right.py.

14.124.3.3 rpki.left_right.parent_elt.bpki_cms_cert = None [static]

Definition at line 674 of file left_right.py.

14.124.3.4 rpki.left_right.parent_elt.bpki_cms_glue = None [static]

Definition at line 675 of file left_right.py.

14.124.3.5 rpki.left_right.parent_elt.bpki_https_cert = None [static]

Definition at line 676 of file left_right.py.

14.124.3.6 rpki.left_right.parent_elt.bpki_https_glue = None [static]

Definition at line 677 of file left_right.py.

14.124.3.7 string rpki.left_right.parent_elt.element_name = "parent" [static]

Definition at line 661 of file left_right.py.

14.124.3.8 tuple rpki.left_right.parent_elt.elements = ("bpki_cms_cert", "bpki_cms_glue", "bpki_https_cert", "bpki_https_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 664 of file left_right.py.

14.124.3.9 tuple rpki.left_right.parent_elt.handles = (("self", self_elt), ("bsc", bsc_elt), ("repository", repository_elt)) [static]

Reimplemented from rpki.left_right.data_elt.

Definition at line 672 of file left_right.py.

14.124.3.10 tuple rpki.left_right.parent_elt.sql_template [static]

Initial value:

```
rpki.sql.template("parent", "parent_id", "parent_handle",
                                  "self_id", "bsc_id", "repository_id",
                                  ("bpki_cms_cert", rpki.x509.X509), ("bpki_cms_
      glue", rpki.x509.X509),
                                  ("bpki_https_cert", rpki.x509.X509), ("bpki_ht
      tps_glue", rpki.x509.X509),
                                  "peer_contact_uri", "sia_base", "sender_name",
       "recipient_name")
```

Definition at line 667 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

14.125 rpki.left_right.report_error_elt Class Reference

Inherits rpki::xml_utils::text_elt, and rpki::left_right::left_right_namespace.

Inherited by irbe_cli.report_error_elt.

Collaboration diagram for rpki.left_right.report_error_elt:

Public Member Functions

- def from_exception

Public Attributes

- error_code
- self_handle
- tag

Static Public Attributes

- tuple attributes = ("tag", "self_handle", "error_code")

  XML attributes for this element.

- string element_name = "report_error"
- error_text = None
- string text_attribute = "error_text"

  Name of the class attribute that holds the text value.

14.125.1 Detailed Description

```
<report_error/> element.
```

Definition at line 1043 of file left_right.py.

14.125.2 Member Function Documentation

14.125.2.1 def rpki.left_right.report_error_elt.from_exception (*cls*, *e*, *self_handle* = `None`, *tag* = `None`)

```
Generate a <report_error/> element from an exception.
```

Definition at line 1055 of file left_right.py.

14.125.3 Member Data Documentation

14.125.3.1 tuple rpki.left_right.report_error_elt.attributes = ("tag", "self_handle", "error_code") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 1049 of file left_right.py.

14.125.3.2 string rpki.left_right.report_error_elt.element_name = "report_error" [static]

Definition at line 1048 of file left_right.py.

14.125.3.3 rpki.left_right.report_error_elt.error_code

Definition at line 1062 of file left_right.py.

14.125.3.4 rpki.left_right.report_error_elt.error_text = None [static]

Definition at line 1052 of file left_right.py.

14.125.3.5 rpki.left_right.report_error_elt.self_handle

Definition at line 1060 of file left_right.py.

14.125.3.6 rpki.left_right.report_error_elt.tag

Definition at line 1061 of file left_right.py.

14.125.3.7 string rpki.left_right.report_error_elt.text_attribute = "error_text" [static]

Name of the class attribute that holds the text value.

Reimplemented from rpki.xml_utils.text_elt.

Definition at line 1050 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

14.126 rpki.left_right.repository_elt Class Reference

Inherits rpki::left_right::data_elt.

Inherited by irbe_cli.repository_elt.

Collaboration diagram for rpki.left_right.repository_elt:

Public Member Functions

- def call_pubd
- def default_pubd_handler
- def parents

Static Public Attributes

- tuple attributes = ("action", "tag", "self_handle", "repository_handle", "bsc_-handle", "peer_contact_uri")

  XML attributes for this element.

- bpki_cert = None
- bpki_glue = None
- string element_name = "repository"
- tuple elements = ("bpki_cert", "bpki_glue")

  XML elements contained by this element.

- tuple handles = (("self", self_elt), ("bsc", bsc_elt))
- tuple sql_template

14.126.1 Detailed Description

```
<repository/> element.
```

Definition at line 573 of file left_right.py.

14.126.2 Member Function Documentation

14.126.2.1 def rpki.left_right.repository_elt.call_pubd (*self*, *callback*, *errback*, *q_msg*, *handlers* = `None`)

```
Send a message to publication daemon and return the response.

As a convenience, attempting to send an empty message returns
immediate success without sending anything.

Handlers is a dict of handler functions to process the response
PDUs.  If the tag value in the response PDU appears in the dict,
the associated handler is called to process the PDU.  If no tag
matches, default_pubd_handler() is called.  A handler value of
False suppresses calling of the default handler.
```

Definition at line 601 of file left_right.py.

14.126.2.2 def rpki.left_right.repository_elt.default_pubd_handler (*pdu*)

```
Default handler for publication response PDUs.
```

Definition at line 595 of file left_right.py.

14.126.2.3 def rpki.left_right.repository_elt.parents (*self*)

```
Fetch all parent objects that link to this repository object.
```

Definition at line 590 of file left_right.py.

14.126.3 Member Data Documentation

14.126.3.1 tuple rpki.left_right.repository_elt.attributes = ("action", "tag", "self_handle", "repository_handle", "bsc_handle", "peer_contact_uri") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 579 of file left_right.py.

14.126.3.2 rpki.left_right.repository_elt.bpki_cert = None [static]

Definition at line 587 of file left_right.py.

14.126.3.3 rpki.left_right.repository_elt.bpki_glue = None [static]

Definition at line 588 of file left_right.py.

14.126.3.4 string rpki.left_right.repository_elt.element_name = "repository" [static]

Definition at line 578 of file left_right.py.

14.126.3.5 tuple rpki.left_right.repository_elt.elements = ("bpki_cert", "bpki_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 580 of file left_right.py.

14.126.3.6 tuple rpki.left_right.repository_elt.handles = (("self", self_elt), ("bsc", bsc_elt)) [static]

Reimplemented from rpki.left_right.data_elt.

Definition at line 585 of file left_right.py.

14.126.3.7 tuple rpki.left_right.repository_elt.sql_template [static]

Initial value:

```
rpki.sql.template("repository", "repository_id", "repository_handle",
                                  "self_id", "bsc_id", "peer_contact_uri",
                                  ("bpki_cert", rpki.x509.X509), ("bpki_glue", r
      pki.x509.X509))
```

Definition at line 582 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

14.127 rpki.left_right.sax_handler Class Reference

Inherits rpki::xml_utils::sax_handler.

Inherited by irbe_cli.left_right_sax_handler.

Collaboration diagram for rpki.left_right.sax_handler:

Static Public Attributes

- string name = "msg"
- pdu = msg
- string version = "1"

14.127.1 Detailed Description

```
SAX handler for Left-Right protocol.
```

Definition at line 1111 of file left_right.py.

14.127.2 Member Data Documentation

14.127.2.1 string rpki.left_right.sax_handler.name = "msg" [static]

Definition at line 1117 of file left_right.py.

14.127.2.2 rpki.left_right.sax_handler.pdu = msg [static]

Reimplemented in irbe_cli.left_right_sax_handler.

Definition at line 1116 of file left_right.py.

14.127.2.3 string rpki.left_right.sax_handler.version = "1" [static]

Definition at line 1118 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

14.128 rpki.left_right.self_elt Class Reference

Inherits rpki::left_right::data_elt.

Inherited by irbe_cli.self_elt.

Collaboration diagram for rpki.left_right.self_elt:

Public Member Functions

- def bscs
- def children
- def client_poll
- def cron
- def parents
- def regenerate_crls_and_manifests
- def repositories
- def roas
- def serve_fetch_all
- def serve_fetch_handle
- def serve_fetch_one_maybe
- def serve_post_save_hook
- def serve_publish_world_now
- def serve_rekey
- def serve_revoke
- def serve_revoke_forgotten
- def serve_run_now
- def update_children
- def update_roas

Static Public Attributes

- tuple attributes = ("action", "tag", "self_handle", "crl_interval", "regen_-margin")

  XML attributes for this element.

- tuple booleans = ("rekey", "reissue", "revoke", "run_now", "publish_world_-now", "revoke_forgotten")

  Boolean attributes (value "yes" or "no") for this element.

- bpki_cert = None
- bpki_glue = None
- crl_interval = None
- string element_name = "self"
- tuple elements = ("bpki_cert", "bpki_glue")

  XML elements contained by this element.

- tuple handles = ()
- regen_margin = None
- tuple sql_template
- use_hsm = False

14.128.1 Detailed Description

```
<self/> element.
```

Definition at line 124 of file left_right.py.

14.128.2 Member Function Documentation

14.128.2.1 def rpki.left_right.self_elt.bscs (*self*)

```
Fetch all BSC objects that link to this self object.
```

Definition at line 145 of file left_right.py.

14.128.2.2 def rpki.left_right.self_elt.children (*self*)

```
Fetch all child objects that link to this self object.
```

Definition at line 157 of file left_right.py.

14.128.2.3 def rpki.left_right.self_elt.client_poll (*self*, *callback*)

```
Run the regular client poll cycle with each of this self's parents
in turn.
```

Definition at line 302 of file left_right.py.

14.128.2.4 def rpki.left_right.self_elt.cron (*self*, *cb*)

```
Periodic tasks.
```

Definition at line 274 of file left_right.py.

14.128.2.5 def rpki.left_right.self_elt.parents (*self*)

```
Fetch all parent objects that link to this self object.
```

Definition at line 153 of file left_right.py.

14.128.2.6 def rpki.left_right.self_elt.regenerate_crls_and_manifests (*self*, *cb*)

```
Generate new CRLs and manifests as necessary for all of this
self's CAs.  Extracting nextUpdate from a manifest is hard at the
moment due to implementation silliness, so for now we generate a
new manifest whenever we generate a new CRL

This method also cleans up tombstones left behind by revoked
ca_detail objects, since we're walking through the relevant
portions of the database anyway.
```

Definition at line 428 of file left_right.py.

14.128.2.7 def rpki.left_right.self_elt.repositories (*self*)

```
Fetch all repository objects that link to this self object.
```

Definition at line 149 of file left_right.py.

14.128.2.8 def rpki.left_right.self_elt.roas (*self*)

```
Fetch all ROA objects that link to this self object.
```

Definition at line 161 of file left_right.py.

14.128.2.9 def rpki.left_right.self_elt.serve_fetch_all (*self*)

```
Find the self objects upon which a list action should operate.
This is different from the list action for all other objects,
where list only works within a given self_id context.
```

Reimplemented from rpki.left_right.data_elt.

Definition at line 266 of file left_right.py.

14.128.2.10 def rpki.left_right.self_elt.serve_fetch_handle (*cls*, *gctx*, *self_id*, *self_handle*)

```
Find a self object based on its self_handle.
```

Reimplemented from rpki.left_right.data_elt.

Definition at line 260 of file left_right.py.

14.128.2.11 def rpki.left_right.self_elt.serve_fetch_one_maybe (*self*)

```
Find the self object upon which a get, set, or destroy action
should operate, or which would conflict with a create method.
```

Reimplemented from rpki.left_right.data_elt.

Definition at line 252 of file left_right.py.

14.128.2.12 def rpki.left_right.self_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Extra server actions for self_elt.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 165 of file left_right.py.

14.128.2.13 def rpki.left_right.self_elt.serve_publish_world_now (*self*, *cb*, *eb*)

```
Handle a left-right publish_world_now action for this self.

The publication stuff needs refactoring, right now publication is
interleaved with local operations in a way that forces far too
many bounces through the task system for any complex update.  The
whole thing ought to be rewritten to queue up outgoing publication
```

```
PDUs and only send them when we're all done or when we need to
force publication at a particular point in a multi-phase operation.

Once that reorganization has been done, this method should be
rewritten to reuse the low-level publish() methods that each
object will have...but we're not there yet.  So, for now, we just
do this via brute force.  Think of it as a trial version to see
whether we've identified everything that needs to be republished
for this operation.
```

Definition at line 213 of file left_right.py.

14.128.2.14 def rpki.left_right.self_elt.serve_rekey (*self*, *cb*, *eb*)

```
Handle a left-right rekey action for this self.
```

Definition at line 186 of file left_right.py.

14.128.2.15 def rpki.left_right.self_elt.serve_revoke (*self*, *cb*, *eb*)

```
Handle a left-right revoke action for this self.
```

Definition at line 195 of file left_right.py.

14.128.2.16 def rpki.left_right.self_elt.serve_revoke_forgotten (*self*, *cb*, *eb*)

```
Handle a left-right revoke_forgotten action for this self.
```

Definition at line 204 of file left_right.py.

14.128.2.17 def rpki.left_right.self_elt.serve_run_now (*self*, *cb*, *eb*)

```
Handle a left-right run_now action for this self.
```

Definition at line 245 of file left_right.py.

14.128.2.18 def rpki.left_right.self_elt.update_children (*self*, *cb*)

```
Check for updated IRDB data for all of this self's children and
issue new certs as necessary.  Must handle changes both in
resources and in expiration date.
```

Definition at line 361 of file left_right.py.

14.128.2.19 def rpki.left_right.self_elt.update_roas (*self*, *cb*)

```
Generate or update ROAs for this self.
```

Definition at line 470 of file left_right.py.

14.128.3 Member Data Documentation

14.128.3.1 tuple rpki.left_right.self_elt.attributes = ("action", "tag", "self_handle", "crl_interval", "regen_margin") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 130 of file left_right.py.

14.128.3.2 tuple rpki.left_right.self_elt.booleans = ("rekey", "reissue", "revoke", "run_now", "publish_world_now", "revoke_forgotten") [static]

Boolean attributes (value "yes" or "no") for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 132 of file left_right.py.

14.128.3.3 rpki.left_right.self_elt.bpki_cert = None [static]

Definition at line 142 of file left_right.py.

14.128.3.4 rpki.left_right.self_elt.bpki_glue = None [static]

Definition at line 143 of file left_right.py.

14.128.3.5 rpki.left_right.self_elt.crl_interval = None [static]

Definition at line 140 of file left_right.py.

14.128.3.6 string rpki.left_right.self_elt.element_name = "self" [static]

Definition at line 129 of file left_right.py.

14.128.3.7 tuple rpki.left_right.self_elt.elements = ("bpki_cert", "bpki_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 131 of file left_right.py.

14.128.3.8 tuple rpki.left_right.self_elt.handles = () [static]

Reimplemented from rpki.left_right.data_elt.

Definition at line 137 of file left_right.py.

14.128.3.9 rpki.left_right.self_elt.regen_margin = None [static]

Definition at line 141 of file left_right.py.

14.128.3.10 tuple rpki.left_right.self_elt.sql_template [static]

Initial value:

```
rpki.sql.template("self", "self_id", "self_handle",
                                  "use_hsm", "crl_interval", "regen_margin",
                                  ("bpki_cert", rpki.x509.X509), ("bpki_glue", r
      pki.x509.X509))
```

Definition at line 134 of file left_right.py.

14.128.3.11 rpki.left_right.self_elt.use_hsm = False [static]

Definition at line 139 of file left_right.py.

The documentation for this class was generated from the following file:

- left_right.py (3191)

14.129 rpki.log.logger Class Reference

Inherits object.

Collaboration diagram for rpki.log.logger:

Public Member Functions

- def __call__
- def __init__

Public Attributes

- priority

14.129.1 Detailed Description

```
Closure for logging.
```

Definition at line 71 of file log.py.

14.129.2 Member Function Documentation

14.129.2.1 def rpki.log.logger.__call__ (*self*, *message*)

Definition at line 79 of file log.py.

14.129.2.2 def rpki.log.logger.__init__ (*self*, *priority*)

Definition at line 76 of file log.py.

14.129.3 Member Data Documentation

14.129.3.1 rpki.log.logger.priority

Definition at line 77 of file log.py.

The documentation for this class was generated from the following file:

- log.py (3107)

14.130 rpki.manifest.FileAndHash Class Reference

Inherits Sequence.

Collaboration diagram for rpki.manifest.FileAndHash:

Public Member Functions

- def __init__

Public Attributes

- file
- hash

14.130.1 Detailed Description

Definition at line 27 of file manifest.py.

14.130.2 Member Function Documentation

14.130.2.1 def rpki.manifest.FileAndHash.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 28 of file manifest.py.

14.130.3 Member Data Documentation

14.130.3.1 rpki.manifest.FileAndHash.file

Definition at line 29 of file manifest.py.

14.130.3.2 rpki.manifest.FileAndHash.hash

Definition at line 30 of file manifest.py.

The documentation for this class was generated from the following file:

- manifest.py (2424)

14.131 rpki.manifest.FilesAndHashes Class Reference

Inherits SequenceOf.

Collaboration diagram for rpki.manifest.FilesAndHashes:

Public Member Functions

- def __init__

14.131.1 Detailed Description

Definition at line 34 of file manifest.py.

14.131.2 Member Function Documentation

14.131.2.1 def rpki.manifest.FilesAndHashes.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 35 of file manifest.py.

The documentation for this class was generated from the following file:

- manifest.py (2424)

14.132 rpki.manifest.Manifest Class Reference

Inherits Sequence.

Collaboration diagram for rpki.manifest.Manifest:

Public Member Functions

- def __init__

Public Attributes

- explicitVersion
- fileHashAlg
- fileList
- manifestNumber
- nextUpdate

- thisUpdate
- version

14.132.1 Detailed Description

Definition at line 38 of file manifest.py.

14.132.2 Member Function Documentation

14.132.2.1 def rpki.manifest.Manifest.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 39 of file manifest.py.

14.132.3 Member Data Documentation

14.132.3.1 rpki.manifest.Manifest.explicitVersion

Definition at line 41 of file manifest.py.

14.132.3.2 rpki.manifest.Manifest.fileHashAlg

Definition at line 45 of file manifest.py.

14.132.3.3 rpki.manifest.Manifest.fileList

Definition at line 46 of file manifest.py.

14.132.3.4 rpki.manifest.Manifest.manifestNumber

Definition at line 42 of file manifest.py.

14.132.3.5 rpki.manifest.Manifest.nextUpdate

Definition at line 44 of file manifest.py.

14.132.3.6 rpki.manifest.Manifest.thisUpdate

Definition at line 43 of file manifest.py.

14.132.3.7 rpki.manifest.Manifest.version

Definition at line 40 of file manifest.py.

The documentation for this class was generated from the following file:

- manifest.py (2424)

14.133 rpki.myrpki.CA Class Reference

Inherits object.

Collaboration diagram for rpki.myrpki.CA:

Public Member Functions

- def __init__
- def bsc
- def cms_xml_sign
- def cms_xml_verify
- def ee

- def fxcert
- def run_ca
- def run_dgst
- def run_openssl
- def run_req
- def setup
- def touch_file
- def xcert

Public Attributes

- cer
- cfg
- crl
- crlnum
- dir
- env
- index
- key
- openssl
- req
- serial

Static Public Attributes

- dictionary path_restriction

14.133.1 Detailed Description

```
Representation of one certification authority.
```

Definition at line 547 of file myrpki.py.

14.133.2 Member Function Documentation

14.133.2.1 def rpki.myrpki.CA.__init__ (*self*, *cfg_file*, *dir*)

Definition at line 558 of file myrpki.py.

14.133.2.2 def rpki.myrpki.CA.bsc (*self*, *pkcs10*)

```
Issue BSC certificiate, if we have a PKCS #10 request for it.
```

Definition at line 711 of file myrpki.py.

14.133.2.3 def rpki.myrpki.CA.cms_xml_sign (*self*, *ee_name*, *base_name*, *elt*)

```
Sign an XML object with CMS, return Base64 text.
```

Definition at line 673 of file myrpki.py.

14.133.2.4 def rpki.myrpki.CA.cms_xml_verify (*self*, *b64*, *ca*)

```
Attempt to verify and extract XML from a Base64-encoded signed CMS
object.  CA is the filename of a certificate that we expect to be
the issuer of the EE certificate bundled with the CMS, and must
previously have been cross-certified under our trust anchor.
```

Definition at line 686 of file myrpki.py.

14.133.2.5 def rpki.myrpki.CA.ee (*self*, *ee_name*, *base_name*)

```
Issue an end-enity certificate.
```

Definition at line 659 of file myrpki.py.

14.133.2.6 def rpki.myrpki.CA.fxcert (*self*, *b64*, *filename* = `None`, *path_restriction* = `0`)

```
Write PEM certificate to file, then cross-certify.
```

Definition at line 732 of file myrpki.py.

14.133.2.7 def rpki.myrpki.CA.run_ca (*self*, *args*)

```
Run OpenSSL "ca" command with common initial arguments.
```

Definition at line 593 of file myrpki.py.

14.133.2.8 def rpki.myrpki.CA.run_dgst (*self*, *input*, *algorithm* = `"md5"`)

```
Run OpenSSL "dgst" command, return cleaned-up result.
```

Definition at line 610 of file myrpki.py.

14.133.2.9 def rpki.myrpki.CA.run_openssl (*self*, *cmd*, *kwargs*)

```
Run an OpenSSL command, suppresses stderr unless OpenSSL returns
failure, and returns stdout.
```

Definition at line 577 of file myrpki.py.

14.133.2.10 def rpki.myrpki.CA.run_req (*self*, *key_file*, *req_file*, *log_key* = `sys.stdout`)

```
Run OpenSSL "genrsa" and  "req" commands.
```

Definition at line 599 of file myrpki.py.

14.133.2.11 def rpki.myrpki.CA.setup (*self*, *ca_name*)

```
Set up this CA.  ca_name is an X.509 distinguished name in
/tag=val/tag=val format.
```

Definition at line 633 of file myrpki.py.

14.133.2.12 def rpki.myrpki.CA.touch_file (*filename*, *content* = `None`)

```
Create dumb little text files expected by OpenSSL "ca" utility.
```

Definition at line 623 of file myrpki.py.

14.133.2.13 def rpki.myrpki.CA.xcert (*self*, *cert*, *path_restriction* = `0`)

```
Cross-certify a certificate represented as a PEM file.
```

Definition at line 745 of file myrpki.py.

14.133.3 Member Data Documentation

14.133.3.1 rpki.myrpki.CA.cer

Definition at line 561 of file myrpki.py.

14.133.3.2 rpki.myrpki.CA.cfg

Definition at line 559 of file myrpki.py.

14.133.3.3 rpki.myrpki.CA.crl

Definition at line 564 of file myrpki.py.

14.133.3.4 rpki.myrpki.CA.crlnum

Definition at line 567 of file myrpki.py.

14.133.3.5 rpki.myrpki.CA.dir

Definition at line 560 of file myrpki.py.

14.133.3.6 rpki.myrpki.CA.env

Definition at line 572 of file myrpki.py.

14.133.3.7 rpki.myrpki.CA.index

Definition at line 565 of file myrpki.py.

14.133.3.8 rpki.myrpki.CA.key

Definition at line 562 of file myrpki.py.

14.133.3.9 rpki.myrpki.CA.openssl

Definition at line 570 of file myrpki.py.

14.133.3.10 dictionary rpki.myrpki.CA.path_restriction [static]

Initial value:

```
{ 0 : "ca_x509_ext_xcert0",
                        1 : "ca_x509_ext_xcert1" }
```

Definition at line 555 of file myrpki.py.

14.133.3.11 rpki.myrpki.CA.req

Definition at line 563 of file myrpki.py.

14.133.3.12 rpki.myrpki.CA.serial

Definition at line 566 of file myrpki.py.

The documentation for this class was generated from the following file:

- myrpki.py

14.134 rpki.myrpki.child Class Reference

Inherits object.

Collaboration diagram for rpki.myrpki.child:

Public Member Functions

- def __init__
- def __repr__
- def add
- def xml

Public Attributes

- asns
- bpki_certificate
- handle
- v4
- v6
- validity

Static Public Attributes

- tuple v4re = re.compile("^(([0-9]{1,3}\.){3}[0-9]{1,3}/[0-9]+)|(([0-9]{1,3}\.){3}[0-9]{1,3}-([0-9]{1,3}\.){3}[0-9]{1,3})$", re.I)
- tuple v6re = re.compile("^(([0-9a-f]{0,4}:){0,15}[0-9a-f]{0,4}/[0-9]+)|(([0-9a-f]{0,4}:){0,15}[0-9a-f]{0,4}-([0-9a-f]{0,4}:){0,15}[0-9a-f]{0,4})$", re.I)

14.134.1 Detailed Description

```
Representation of one child entity.
```

Definition at line 184 of file myrpki.py.

14.134.2 Member Function Documentation

14.134.2.1 def rpki.myrpki.child.__init__ (*self*, *handle*)

Definition at line 192 of file myrpki.py.

14.134.2.2 def rpki.myrpki.child.__repr__ (*self*)

Definition at line 200 of file myrpki.py.

14.134.2.3 def rpki.myrpki.child.add (*self*, *prefix* = `None`, *asn* = `None`, *validity* = `None`, *bpki_certificate* = `None`)

```
Add prefix, autonomous system number, validity date, or BPKI
certificate for this child.
```

Definition at line 214 of file myrpki.py.

14.134.2.4 def rpki.myrpki.child.xml (*self*, *e*)

```
Render this child as an XML element.
```

Definition at line 233 of file myrpki.py.

14.134.3 Member Data Documentation

14.134.3.1 rpki.myrpki.child.asns

Definition at line 194 of file myrpki.py.

14.134.3.2 rpki.myrpki.child.bpki_certificate

Definition at line 198 of file myrpki.py.

14.134.3.3 rpki.myrpki.child.handle

Definition at line 193 of file myrpki.py.

14.134.3.4 rpki.myrpki.child.v4

Definition at line 195 of file myrpki.py.

14.134.3.5 tuple rpki.myrpki.child.v4re = re.compile("^(([0-9]{1,3}\.){3}[0-9]{1,3}/[0-9]+)|(([0-9]{1,3}\.){3}[0-9]{1,3}-([0-9]{1,3}\.){3}[0-9]{1,3})$", re.I) [static]

Definition at line 189 of file myrpki.py.

14.134.3.6 rpki.myrpki.child.v6

Definition at line 196 of file myrpki.py.

14.134.3.7 tuple rpki.myrpki.child.v6re = re.compile("^(([0-9a-f]{0,4}:){0,15}[0-9a-f]{0,4}/[0-9]+)|(([0-9a-f]{0,4}:){0,15}[0-9a-f]{0,4}-([0-9a-f]{0,4}:){0,15}[0-9a-f]{0,4})$", re.I) [static]

Definition at line 190 of file myrpki.py.

14.134.3.8 rpki.myrpki.child.validity

Definition at line 197 of file myrpki.py.

The documentation for this class was generated from the following file:

- myrpki.py

14.135 rpki.myrpki.children Class Reference

Inherits dict.

Collaboration diagram for rpki.myrpki.children:

Public Member Functions

- def add
- def from_csv
- def xml

14.135.1 Detailed Description

```
Database of children.
```

Definition at line 251 of file myrpki.py.

14.135.2 Member Function Documentation

14.135.2.1 def rpki.myrpki.children.add (*self*, *handle*, *prefix* = `None`, *asn* = `None`, *validity* = `None`, *bpki_certificate* = `None`)

```
Add resources to a child, creating the child object if necessary.
```

Definition at line 256 of file myrpki.py.

14.135.2.2 def rpki.myrpki.children.from_csv (*cls*, *prefix_csv_file*, *asn_csv_file*, *fxcert*, *entitydb*)

```
Parse child resources, certificates, and validity dates from CSV files.
```

Definition at line 272 of file myrpki.py.

14.135.2.3 def rpki.myrpki.children.xml (*self*, *e*)

```
Render children database to XML.
```

Definition at line 264 of file myrpki.py.

The documentation for this class was generated from the following file:

- myrpki.py

14.136 rpki.myrpki.comma_set Class Reference

Inherits set.

Collaboration diagram for rpki.myrpki.comma_set:

Public Member Functions

- def __str__

14.136.1 Detailed Description

```
Minor customization of set(), to provide a print syntax.
```

Definition at line 86 of file myrpki.py.

14.136.2 Member Function Documentation

14.136.2.1 def rpki.myrpki.comma_set.__str__ (*self*)

Definition at line 91 of file myrpki.py.

The documentation for this class was generated from the following file:

- myrpki.py

14.137 rpki.myrpki.csv_reader Class Reference

Inherits object.

Collaboration diagram for rpki.myrpki.csv_reader:

Public Member Functions

- def __init__
- def __iter__

Public Attributes

- columns
- comment_characters
- file
- filename
- min_columns

14.137.1 Detailed Description

```
Reader for tab-delimited text that's (slightly) friendlier than the
stock Python csv module (which isn't intended for direct use by
humans anyway, and neither was this package originally, but that
seems to be the way that it has evolved...).

Columns parameter specifies how many columns users of the reader
expect to see; lines with fewer columns will be padded with None
values.

Original API design for this class courtesy of Warren Kumari, but
don't blame him if you don't like what I did with his ideas.
```

Definition at line 478 of file myrpki.py.

14.137.2 Member Function Documentation

14.137.2.1 def rpki.myrpki.csv_reader.__init__ (*self*, *filename*, *columns* = `None`, *min_columns* = `None`, *comment_characters* = `"#;"`)

Definition at line 493 of file myrpki.py.

14.137.2.2 def rpki.myrpki.csv_reader.__iter__ (*self*)

Definition at line 504 of file myrpki.py.

14.137.3 Member Data Documentation

14.137.3.1 rpki.myrpki.csv_reader.columns

Definition at line 499 of file myrpki.py.

14.137.3.2 rpki.myrpki.csv_reader.comment_characters

Definition at line 501 of file myrpki.py.

14.137.3.3 rpki.myrpki.csv_reader.file

Definition at line 502 of file myrpki.py.

14.137.3.4 rpki.myrpki.csv_reader.filename

Definition at line 498 of file myrpki.py.

14.137.3.5 rpki.myrpki.csv_reader.min_columns

Definition at line 500 of file myrpki.py.

The documentation for this class was generated from the following file:

- myrpki.py

14.138 rpki.myrpki.EntityDB Class Reference

Inherits object.

Collaboration diagram for rpki.myrpki.EntityDB:

Public Member Functions

- def __call__
- def __init__
- def iterate

Public Attributes

- dir

14.138.1 Detailed Description

```
Wrapper for entitydb path lookups.  Hmm, maybe some or all of the
entitydb glob stuff should end up here too?  Later.
```

Definition at line 94 of file myrpki.py.

14.138.2 Member Function Documentation

14.138.2.1 def rpki.myrpki.EntityDB.__call__ (*self*, *args*)

Definition at line 103 of file myrpki.py.

14.138.2.2 def rpki.myrpki.EntityDB.__init__ (*self*, *cfg*)

Definition at line 100 of file myrpki.py.

14.138.2.3 def rpki.myrpki.EntityDB.iterate (*self*, *args*)

Definition at line 106 of file myrpki.py.

14.138.3 Member Data Documentation

14.138.3.1 rpki.myrpki.EntityDB.dir

Definition at line 101 of file myrpki.py.

The documentation for this class was generated from the following file:

- myrpki.py

14.139 rpki.myrpki.main Class Reference

Inherits rpki::cli::Cmd.

Collaboration diagram for rpki.myrpki.main:

Public Member Functions

- def __init__
- def configure_resources_main
- def do_configure_child
- def do_configure_daemons
- def do_configure_parent

- def do_configure_publication_client
- def do_configure_repository
- def do_configure_resources
- def do_initialize
- def help_overview
- def read_config

Public Attributes

- bpki_resources
- bpki_servers
- cfg
- cfg_file
- entitydb
- handle
- histfile
- pubd_contact_info
- rsync_module
- rsync_server
- run_pubd
- run_rootd
- run_rpkid

Static Public Attributes

- completedefault = rpki.cli.Cmd.filename_complete
- string prompt = "myrpki> "
- show_xml = False

14.139.1 Detailed Description

Definition at line 851 of file myrpki.py.

14.139.2 Member Function Documentation

14.139.2.1 def rpki.myrpki.main.__init__ (*self*)

Definition at line 859 of file myrpki.py.

14.139.2.2 def rpki.myrpki.main.configure_resources_main (*self*, *msg* = `None`)

```
Main program of old myrpki.py script.  This remains separate
because it's called from more than one place.
```

Definition at line 1230 of file myrpki.py.

14.139.2.3 def rpki.myrpki.main.do_configure_child (*self*, *arg*)

```
Configure a new child of this RPKI entity, given the child's XML
identity file as an input.  This command extracts the child's data
from the XML, cross-certifies the child's resource-holding BPKI
certificate, and generates an XML file describing the relationship
between the child and this parent, including this parent's BPKI
data and up-down protocol service URI.
```

Definition at line 997 of file myrpki.py.

14.139.2.4 def rpki.myrpki.main.do_configure_daemons (*self*, *arg*)

```
Configure RPKI daemons with the data built up by the other
commands in this program.

The basic model here is that each entity with resources to certify
runs the myrpki tool, but not all of them necessarily run their
own RPKI engines.  The entities that do run RPKI engines get data
from the entities they host via the XML files output by the
configure_resources command.  Those XML files are the input to
this command, which uses them to do all the work of configuring
daemons, populating SQL databases, and so forth.  A few operations
(eg, BSC construction) generate data which has to be shipped back
to the resource holder, which we do by updating the same XML file.

In essence, the XML files are a sneakernet (or email, or carrier
pigeon) communication channel between the resource holders and the
RPKI engine operators.

As a convenience, for the normal case where the RPKI engine
operator is itself a resource holder, this command in effect runs
the configure_resources command automatically to process the RPKI
engine operator's own resources.

Note that, due to the back and forth nature of some of these
operations, it may take several cycles for data structures to stablize
and everything to reach a steady state.  This is normal.
```

Definition at line 1298 of file myrpki.py.

14.139.2.5 def rpki.myrpki.main.do_configure_parent (*self*, *arg*)

```
Configure a new parent of this RPKI entity, given the output of
the parent's configure_child command as input.  This command reads
the parent's response XML, extracts the parent's BPKI and service
URI information, cross-certifies the parent's BPKI data into this
entity's BPKI, and checks for offers or referrals of publication
service.  If a publication offer or referral is present, we
generate a request-for-service message to that repository, in case
the user wants to avail herself of the referral or offer.
```

Definition at line 1079 of file myrpki.py.

14.139.2.6 def rpki.myrpki.main.do_configure_publication_client (*self*, *arg*)

```
Configure publication server to know about a new client, given the
client's request-for-service message as input.  This command reads
the client's request for service, cross-certifies the client's
BPKI data, and generates a response message containing the
repository's BPKI data and service URI.
```

Definition at line 1126 of file myrpki.py.

14.139.2.7 def rpki.myrpki.main.do_configure_repository (*self*, *arg*)

```
Configure a publication repository for this RPKI entity, given the
repository's response to our request-for-service message as input.
This command reads the repository's response, extracts and
cross-certifies the BPKI data and service URI, and links the
repository data with the corresponding parent data in our local
database.
```

Definition at line 1203 of file myrpki.py.

14.139.2.8 def rpki.myrpki.main.do_configure_resources (*self*, *arg*)

```
Read CSV files and all the descriptions of parents and children
that we've built up, package the result up as a single XML file to
be shipped to a hosting rpkid.
```

Definition at line 1285 of file myrpki.py.

14.139.2.9 def rpki.myrpki.main.do_initialize (*self*, *arg*)

```
Initialize an RPKI installation.  This command reads the
configuration file, creates the BPKI and EntityDB directories,
generates the initial BPKI certificates, and creates an XML file
describing the resource-holding aspect of this RPKI installation.
```

Definition at line 915 of file myrpki.py.

14.139.2.10 def rpki.myrpki.main.help_overview (*self*)

```
Show program __doc__ string.  Perhaps there's some clever way to
do this using the textwrap module, but for now something simple
and crude will suffice.
```

Definition at line 881 of file myrpki.py.

14.139.2.11 def rpki.myrpki.main.read_config (*self*)

Definition at line 891 of file myrpki.py.

14.139.3 Member Data Documentation

14.139.3.1 rpki.myrpki.main.bpki_resources

Definition at line 905 of file myrpki.py.

14.139.3.2 rpki.myrpki.main.bpki_servers

Definition at line 907 of file myrpki.py.

14.139.3.3 rpki.myrpki.main.cfg

Definition at line 893 of file myrpki.py.

14.139.3.4 rpki.myrpki.main.cfg_file

Definition at line 865 of file myrpki.py.

14.139.3.5 rpki.myrpki.main.completedefault = rpki.cli.Cmd.filename_-complete [static]

Definition at line 855 of file myrpki.py.

14.139.3.6 rpki.myrpki.main.entitydb

Definition at line 900 of file myrpki.py.

14.139.3.7 rpki.myrpki.main.handle

Definition at line 896 of file myrpki.py.

14.139.3.8 rpki.myrpki.main.histfile

Reimplemented from rpki.cli.Cmd.

Definition at line 895 of file myrpki.py.

14.139.3.9 string rpki.myrpki.main.prompt = "myrpki> " [static]

Definition at line 853 of file myrpki.py.

14.139.3.10 rpki.myrpki.main.pubd_contact_info

Definition at line 909 of file myrpki.py.

14.139.3.11 rpki.myrpki.main.rsync_module

Definition at line 911 of file myrpki.py.

14.139.3.12 rpki.myrpki.main.rsync_server

Definition at line 912 of file myrpki.py.

14.139.3.13 rpki.myrpki.main.run_pubd

Definition at line 898 of file myrpki.py.

14.139.3.14 rpki.myrpki.main.run_rootd

Definition at line 899 of file myrpki.py.

14.139.3.15 rpki.myrpki.main.run_rpkid

Definition at line 897 of file myrpki.py.

14.139.3.16 rpki.myrpki.main.show_xml = False `[static]`

Definition at line 857 of file myrpki.py.

The documentation for this class was generated from the following file:

- myrpki.py

14.140 rpki.myrpki.parent Class Reference

Inherits object.

Collaboration diagram for rpki.myrpki.parent:

Public Member Functions

- def __init__
- def __repr__
- def add
- def xml

Public Attributes

- bpki_cms_certificate
- bpki_https_certificate
- handle

- myhandle
- service_uri
- sia_base

14.140.1 Detailed Description

```
Representation of one parent entity.
```

Definition at line 290 of file myrpki.py.

14.140.2 Member Function Documentation

14.140.2.1 def rpki.myrpki.parent.__init__ (*self*, *handle*)

Definition at line 295 of file myrpki.py.

14.140.2.2 def rpki.myrpki.parent.__repr__ (*self*)

Definition at line 303 of file myrpki.py.

14.140.2.3 def rpki.myrpki.parent.add (*self*, *service_uri* = `None`, *bpki_cms_certificate* = `None`, *bpki_https_certificate* = `None`, *myhandle* = `None`, *sia_base* = `None`)

```
Add service URI or BPKI certificates to this parent object.
```

Definition at line 317 of file myrpki.py.

14.140.2.4 def rpki.myrpki.parent.xml (*self*, *e*)

```
Render this parent object to XML.
```

Definition at line 336 of file myrpki.py.

14.140.3 Member Data Documentation

14.140.3.1 rpki.myrpki.parent.bpki_cms_certificate

Definition at line 298 of file myrpki.py.

14.140.3.2 rpki.myrpki.parent.bpki_https_certificate

Definition at line 299 of file myrpki.py.

14.140.3.3 rpki.myrpki.parent.handle

Definition at line 296 of file myrpki.py.

14.140.3.4 rpki.myrpki.parent.myhandle

Definition at line 300 of file myrpki.py.

14.140.3.5 rpki.myrpki.parent.service_uri

Definition at line 297 of file myrpki.py.

14.140.3.6 rpki.myrpki.parent.sia_base

Definition at line 301 of file myrpki.py.

The documentation for this class was generated from the following file:

- myrpki.py

14.141 rpki.myrpki.parents Class Reference

Inherits dict.

Collaboration diagram for rpki.myrpki.parents:

Public Member Functions

- def add
- def from_csv
- def xml

14.141.1 Detailed Description

```
Database of parent objects.
```

Definition at line 355 of file myrpki.py.

14.141.2 Member Function Documentation

14.141.2.1 def rpki.myrpki.parents.add (*self*, *handle*, *service_uri* = `None`, *bpki_cms_certificate* = `None`, *bpki_https_certificate* = `None`, *myhandle* = `None`, *sia_base* = `None`)

```
Add service URI or certificates to parent object, creating it if necessary.
```

Definition at line 360 of file myrpki.py.

14.141.2.2 def rpki.myrpki.parents.from_csv (*cls*, *fxcert*, *entitydb*)

```
Parse parent data from entitydb.
```

Definition at line 382 of file myrpki.py.

14.141.2.3 def rpki.myrpki.parents.xml (*self*, *e*)

Definition at line 377 of file myrpki.py.

The documentation for this class was generated from the following file:

- myrpki.py

14.142 rpki.myrpki.repositories Class Reference

Inherits dict.

Collaboration diagram for rpki.myrpki.repositories:

Public Member Functions

- def add
- def from_csv
- def xml

14.142.1 Detailed Description

```
Database of repository objects.
```

Definition at line 443 of file myrpki.py.

14.142.2 Member Function Documentation

14.142.2.1 def rpki.myrpki.repositories.add (*self*, *handle*, *service_uri* = `None`, *bpki_certificate* = `None`)

```
Add service URI or certificate to repository object, creating it if necessary.
```

Definition at line 448 of file myrpki.py.

14.142.2.2 def rpki.myrpki.repositories.from_csv (*cls*, *fxcert*, *entitydb*)

```
Parse repository data from entitydb.
```

Definition at line 464 of file myrpki.py.

14.142.2.3 def rpki.myrpki.repositories.xml (*self*, *e*)

Definition at line 459 of file myrpki.py.

The documentation for this class was generated from the following file:

- myrpki.py

14.143 rpki.myrpki.repository Class Reference

Inherits object.

Collaboration diagram for rpki.myrpki.repository:

Public Member Functions

- def __init__
- def __repr__
- def add
- def xml

Public Attributes

- bpki_certificate
- handle
- service_uri

14.143.1 Detailed Description

```
Representation of one repository entity.
```

Definition at line 401 of file myrpki.py.

14.143.2 Member Function Documentation

14.143.2.1 def rpki.myrpki.repository.__init__ (*self*, *handle*)

Definition at line 406 of file myrpki.py.

14.143.2.2 def rpki.myrpki.repository.__repr__ (*self*)

Definition at line 411 of file myrpki.py.

14.143.2.3 def rpki.myrpki.repository.add (*self*, *service_uri* = `None`, *bpki_certificate* = `None`)

```
Add service URI or BPKI certificates to this repository object.
```

Definition at line 419 of file myrpki.py.

14.143.2.4 def rpki.myrpki.repository.xml (*self*, *e*)

```
Render this repository object to XML.
```

Definition at line 428 of file myrpki.py.

14.143.3 Member Data Documentation

14.143.3.1 rpki.myrpki.repository.bpki_certificate

Definition at line 409 of file myrpki.py.

14.143.3.2 rpki.myrpki.repository.handle

Definition at line 407 of file myrpki.py.

14.143.3.3 rpki.myrpki.repository.service_uri

Definition at line 408 of file myrpki.py.

The documentation for this class was generated from the following file:

- myrpki.py

14.144 rpki.myrpki.roa_request Class Reference

Inherits object.

Collaboration diagram for rpki.myrpki.roa_request:

Public Member Functions

- def __init__
- def __repr__
- def add
- def xml

Public Attributes

- asn

- group
- v4
- v6

Static Public Attributes

- tuple v4re = re.compile("^([0-9]{1,3}\.){3}[0-9]{1,3}/[0-9]+(-[0-9]+)?$", re.I)
- tuple v6re = re.compile("^([0-9a-f]{0,4}:){0,15}[0-9a-f]{0,4}/[0-9]+(-[0-9]+)?$", re.I)

14.144.1 Detailed Description

```
Representation of a ROA request.
```

Definition at line 109 of file myrpki.py.

14.144.2 Member Function Documentation

14.144.2.1 def rpki.myrpki.roa_request.__init__ (*self*, *asn*, *group*)

Definition at line 117 of file myrpki.py.

14.144.2.2 def rpki.myrpki.roa_request.__repr__ (*self*)

Definition at line 123 of file myrpki.py.

14.144.2.3 def rpki.myrpki.roa_request.add (*self*, *prefix*)

```
Add one prefix to this ROA request.
```

Definition at line 131 of file myrpki.py.

14.144.2.4 def rpki.myrpki.roa_request.xml (*self*, *e*)

```
Generate XML element represeting representing this ROA request.
```

Definition at line 142 of file myrpki.py.

14.144.3 Member Data Documentation

14.144.3.1 rpki.myrpki.roa_request.asn

Definition at line 118 of file myrpki.py.

14.144.3.2 rpki.myrpki.roa_request.group

Definition at line 119 of file myrpki.py.

14.144.3.3 rpki.myrpki.roa_request.v4

Definition at line 120 of file myrpki.py.

14.144.3.4 tuple rpki.myrpki.roa_request.v4re = re.compile("^([0-9]{1,3}\.){3}[0-9]{1,3}/[0-9]+(-[0-9]+)?$", re.I) [static]

Definition at line 114 of file myrpki.py.

14.144.3.5 rpki.myrpki.roa_request.v6

Definition at line 121 of file myrpki.py.

14.144.3.6 tuple rpki.myrpki.roa_request.v6re = re.compile("^([0-9a-f]{0,4}:){0,15}[0-9a-f]{0,4}/[0-9]+(-[0-9]+)?$", re.I) [static]

Definition at line 115 of file myrpki.py.

The documentation for this class was generated from the following file:

- myrpki.py

14.145 rpki.myrpki.roa_requests Class Reference

Inherits dict.

Collaboration diagram for rpki.myrpki.roa_requests:

Public Member Functions

- def add
- def from_csv
- def xml

14.145.1 Detailed Description

```
Database of ROA requests.
```

Definition at line 152 of file myrpki.py.

14.145.2 Member Function Documentation

14.145.2.1 def rpki.myrpki.roa_requests.add (*self*, *asn*, *group*, *prefix*)

```
Add one <ASN, group, prefix> set to ROA request database.
```

Definition at line 157 of file myrpki.py.

14.145.2.2 def rpki.myrpki.roa_requests.from_csv (*cls*, *roa_csv_file*)

```
Parse ROA requests from CSV file.
```

Definition at line 174 of file myrpki.py.

14.145.2.3 def rpki.myrpki.roa_requests.xml (*self*, *e*)

```
Render ROA requests as XML elements.
```

Definition at line 166 of file myrpki.py.

The documentation for this class was generated from the following file:

- myrpki.py

14.146 rpki.publication.certificate_elt Class Reference

Inherits rpki::publication::publication_object_elt.

Inherited by irbe_cli.certificate_elt.

Collaboration diagram for rpki.publication.certificate_elt:

Static Public Attributes

- string element_name = "certificate"
- payload_type = rpki.x509.X509

14.146.1 Detailed Description

`<certificate/> element.`

Definition at line 287 of file publication.py.

14.146.2 Member Data Documentation

14.146.2.1 string rpki.publication.certificate_elt.element_name = "certificate" [static]

Definition at line 292 of file publication.py.

14.146.2.2 rpki.publication.certificate_elt.payload_type = rpki.x509.X509 [static]

Reimplemented from rpki.publication.publication_object_elt.

Definition at line 293 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

14.147 rpki.publication.client_elt Class Reference

Inherits rpki::publication::control_elt.

Inherited by irbe_cli.client_elt.

Collaboration diagram for rpki.publication.client_elt:

Public Member Functions

- def check_allowed_uri
- def endElement
- def serve_fetch_all
- def serve_fetch_one_maybe
- def serve_post_save_hook

Static Public Attributes

- tuple attributes = ("action", "tag", "client_handle", "base_uri")

  XML attributes for this element.

- base_uri = None
- bpki_cert = None
- bpki_glue = None
- clear_https_ta_cache = False
- string element_name = "client"
- tuple elements = ("bpki_cert", "bpki_glue")

  XML elements contained by this element.

- tuple sql_template = rpki.sql.template("client", "client_id", "client_handle", "base_uri", ("bpki_cert", rpki.x509.X509), ("bpki_glue", rpki.x509.X509))

14.147.1 Detailed Description

```
<client/> element.
```

Definition at line 113 of file publication.py.

14.147.2 Member Function Documentation

14.147.2.1 def rpki.publication.client_elt.check_allowed_uri (*self*, *uri*)

Definition at line 160 of file publication.py.

14.147.2.2 def rpki.publication.client_elt.endElement (*self*, *stack*, *name*, *text*)

```
Handle subelements of <client/> element.  These require special
handling because modifying them invalidates the HTTPS trust anchor
cache.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 130 of file publication.py.

14.147.2.3 def rpki.publication.client_elt.serve_fetch_all (*self*)

```
Find client objects on which a list method should operate.
```

Definition at line 156 of file publication.py.

14.147.2.4 def rpki.publication.client_elt.serve_fetch_one_maybe (*self*)

```
Find the client object on which a get, set, or destroy method
should operate, or which would conflict with a create method.
```

Definition at line 149 of file publication.py.

14.147.2.5 def rpki.publication.client_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Extra server actions for client_elt.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 140 of file publication.py.

14.147.3 Member Data Documentation

14.147.3.1 tuple rpki.publication.client_elt.attributes = ("action", "tag", "client_handle", "base_uri") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 119 of file publication.py.

14.147.3.2 rpki.publication.client_elt.base_uri = None [static]

Definition at line 124 of file publication.py.

14.147.3.3 rpki.publication.client_elt.bpki_cert = None [static]

Definition at line 125 of file publication.py.

14.147.3.4 rpki.publication.client_elt.bpki_glue = None [static]

Definition at line 126 of file publication.py.

14.147.3.5 rpki.publication.client_elt.clear_https_ta_cache = False [static]

Definition at line 128 of file publication.py.

14.147.3.6 string rpki.publication.client_elt.element_name = "client" [static]

Definition at line 118 of file publication.py.

14.147.3.7 tuple rpki.publication.client_elt.elements = ("bpki_cert", "bpki_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 120 of file publication.py.

14.147.3.8 tuple rpki.publication.client_elt.sql_template = rpki.sql.template("client", "client_id", "client_handle", "base_uri", ("bpki_cert", rpki.x509.X509), ("bpki_glue", rpki.x509.X509)) [static]

Definition at line 122 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

14.148 rpki.publication.cms_msg Class Reference

Inherits rpki::x509::XML_CMS_object.

Inherited by irbe_cli.publication_cms_msg.

Collaboration diagram for rpki.publication.cms_msg:

Static Public Attributes

- string encoding = "us-ascii"
- saxify = sax_handler.saxify
- schema = rpki.relaxng.publication

14.148.1 Detailed Description

```
Class to hold a CMS-signed publication PDU.
```

Definition at line 415 of file publication.py.

14.148.2 Member Data Documentation

14.148.2.1 string rpki.publication.cms_msg.encoding = "us-ascii" [static]

Definition at line 420 of file publication.py.

14.148.2.2 rpki.publication.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented in irbe_cli.publication_cms_msg.

Definition at line 422 of file publication.py.

14.148.2.3 rpki.publication.cms_msg.schema = rpki.relaxng.publication [static]

Definition at line 421 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

14.149 rpki.publication.config_elt Class Reference

Inherits rpki::publication::control_elt.

Inherited by irbe_cli.config_elt.

Collaboration diagram for rpki.publication.config_elt:

Public Member Functions

- def fetch
- def serve_fetch_one_maybe
- def serve_set
- def startElement

Public Attributes

- config_id

Static Public Attributes

- tuple attributes = ("action", "tag")

  XML attributes for this element.

- string element_name = "config"
- tuple elements = ("bpki_crl",)

  XML elements contained by this element.

- tuple sql_template = rpki.sql.template("config", "config_id", ("bpki_crl", rpki.x509.CRL))
- int wired_in_config_id = 1

14.149.1 Detailed Description

```
<config/> element.  This is a little weird because there should
never be more than one row in the SQL config table, but we have to
put the BPKI CRL somewhere and SQL is the least bad place available.

So we reuse a lot of the SQL machinery, but we nail config_id at 1,
we don't expose it in the XML protocol, and we only support the get
and set actions.
```

Definition at line 61 of file publication.py.

14.149.2 Member Function Documentation

14.149.2.1 def rpki.publication.config_elt.fetch (*cls*, *gctx*)

```
Fetch the config object from SQL.  This requires special handling
because of the weird way we treat config_id.
```

Definition at line 89 of file publication.py.

14.149.2.2 def rpki.publication.config_elt.serve_fetch_one_maybe (*self*)

```
Find the config object on which a get or set method should
operate.
```

Definition at line 106 of file publication.py.

14.149.2.3 def rpki.publication.config_elt.serve_set (*self*, *r_msg*, *cb*, *eb*)

```
Handle a set action.  This requires special handling because
config doesn't support the create method.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 96 of file publication.py.

14.149.2.4 def rpki.publication.config_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
StartElement() handler for config object.  This requires special
handling because of the weird way we treat config_id.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 80 of file publication.py.

14.149.3 Member Data Documentation

14.149.3.1 tuple rpki.publication.config_elt.attributes = ("action", "tag") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 72 of file publication.py.

14.149.3.2 rpki.publication.config_elt.config_id

Definition at line 86 of file publication.py.

14.149.3.3 string rpki.publication.config_elt.element_name = "config" [static]

Definition at line 73 of file publication.py.

14.149.3.4 tuple rpki.publication.config_elt.elements = ("bpki_crl",) [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 74 of file publication.py.

14.149.3.5 tuple rpki.publication.config_elt.sql_template = rpki.sql.template("config", "config_id", ("bpki_crl", rpki.x509.CRL)) [static]

Definition at line 76 of file publication.py.

14.149.3.6 int rpki.publication.config_elt.wired_in_config_id = 1 [static]

Definition at line 78 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

14.150 rpki.publication.control_elt Class Reference

Inherits rpki::xml_utils::data_elt, rpki::sql::sql_persistent, and rpki::publication::publication_namespace.

Inherited by rpki.publication.client_elt, and rpki.publication.config_elt.

Collaboration diagram for rpki.publication.control_elt:

Public Member Functions

- def serve_dispatch

14.150.1 Detailed Description

```
Virtual class for control channel objects.
```

Definition at line 47 of file publication.py.

14.150.2 Member Function Documentation

14.150.2.1 def rpki.publication.control_elt.serve_dispatch (*self*, *r_msg*, *cb*, *eb*)

```
Action dispatch handler.  This needs special handling because we
need to make sure that this PDU arrived via the control channel.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 52 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

14.151 rpki.publication.crl_elt Class Reference

Inherits rpki::publication::publication_object_elt.

Inherited by irbe_cli.crl_elt.

Collaboration diagram for rpki.publication.crl_elt:

Static Public Attributes

- string element_name = "crl"
- payload_type = rpki.x509.CRL

14.151.1 Detailed Description

`<crl/> element.`

Definition at line 295 of file publication.py.

14.151.2 Member Data Documentation

14.151.2.1 string rpki.publication.crl_elt.element_name = "crl" [static]

Definition at line 300 of file publication.py.

14.151.2.2 rpki.publication.crl_elt.payload_type = rpki.x509.CRL [static]

Reimplemented from rpki.publication.publication_object_elt.

Definition at line 301 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

14.152 rpki.publication.manifest_elt Class Reference

Inherits rpki::publication::publication_object_elt.

Inherited by irbe_cli.manifest_elt.

Collaboration diagram for rpki.publication.manifest_elt:

Static Public Attributes

- string element_name = "manifest"
- payload_type = rpki.x509.SignedManifest

14.152.1 Detailed Description

```
<manifest/> element.
```

Definition at line 303 of file publication.py.

14.152.2 Member Data Documentation

14.152.2.1 string rpki.publication.manifest_elt.element_name = "manifest" [static]

Definition at line 308 of file publication.py.

14.152.2.2 rpki.publication.manifest_elt.payload_type = rpki.x509.SignedManifest [static]

Reimplemented from rpki.publication.publication_object_elt.

Definition at line 309 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

14.153 rpki.publication.msg Class Reference

Inherits rpki::xml_utils::msg, and rpki::publication::publication_namespace.

Inherited by irbe_cli.publication_msg.

Collaboration diagram for rpki.publication.msg:

Public Member Functions

- def serve_top_level

Static Public Attributes

- tuple pdus

  Dispatch table of PDUs for this protocol.

- int version = 1

  Protocol version.

14.153.1 Detailed Description

```
Publication PDU.
```

Definition at line 362 of file publication.py.

14.153.2 Member Function Documentation

14.153.2.1 def rpki.publication.msg.serve_top_level (*self*, *gctx*, *client*, *cb*)

```
Serve one msg PDU.
```

Definition at line 376 of file publication.py.

14.153.3 Member Data Documentation

14.153.3.1 rpki::publication.msg::pdus [static]

Initial value:

```
dict((x.element_name, x)
              for x in (config_elt, client_elt, certificate_elt, crl_elt, manifes
      t_elt, roa_elt, report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented in irbe_cli.publication_msg.

Definition at line 373 of file publication.py.

14.153.3.2 rpki::publication.msg::version = 1 [static]

Protocol version.

Reimplemented from rpki.xml_utils.msg.

Definition at line 369 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

14.154 rpki.publication.publication_namespace Class Reference

Inherits object.

Inherited by rpki.publication.control_elt, rpki.publication.msg, rpki.publication.publication_object_elt, and rpki.publication.report_error_elt.

Collaboration diagram for rpki.publication.publication_namespace:

Static Public Attributes

- dictionary nsmap = { None : xmlns }
- string xmlns = "http://www.hactrn.net/uris/rpki/publication-spec/"

14.154.1 Detailed Description

```
XML namespace parameters for publication protocol.
```

Definition at line 39 of file publication.py.

14.154.2 Member Data Documentation

14.154.2.1 dictionary rpki.publication.publication_namespace.nsmap = { None : xmlns } [static]

Definition at line 45 of file publication.py.

14.154.2.2 string rpki.publication.publication_namespace.xmlns = "http://www.hactrn.net/uris/rpki/publication-spec/" [static]

Definition at line 44 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

14.155 rpki.publication.publication_object_elt Class Reference

Inherits rpki::xml_utils::base_elt, and rpki::publication::publication_namespace.

Inherited by rpki.publication.certificate_elt, rpki.publication.crl_elt, rpki.publication.manifest_elt, and rpki.publication.roa_elt.

Collaboration diagram for rpki.publication.publication_object_elt:

Public Member Functions

- def endElement
- def make_publish
- def make_withdraw
- def raise_if_error
- def serve_dispatch
- def serve_publish
- def serve_withdraw
- def toXML
- def uri_to_filename

Static Public Attributes

- tuple attributes = ("action", "tag", "client_handle", "uri")

  XML attributes for this element.

- payload = None
- payload_type = None

14.155.1 Detailed Description

```
Virtual class for publishable objects.  These have very similar
syntax, differences lie in underlying datatype and methods.  XML
methods are a little different from the pattern used for objects
that support the create/set/get/list/destroy actions, but
publishable objects don't go in SQL either so these classes would be
different in any case.
```

Definition at line 164 of file publication.py.

14.155.2 Member Function Documentation

14.155.2.1 def rpki.publication.publication_object_elt.endElement (*self*, *stack*, *name*, *text*)

```
Handle a publishable element element.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 178 of file publication.py.

14.155.2.2 def rpki.publication.publication_object_elt.make_publish (*cls*, *uri*, *obj*, *tag* = `None`)

```
Construct a publication PDU.
```

Definition at line 266 of file publication.py.

14.155.2.3 def rpki.publication.publication_object_elt.make_withdraw (*cls*, *uri*, *obj*, *tag* = `None`)

```
Construct a withdrawal PDU.
```

Definition at line 274 of file publication.py.

14.155.2.4 def rpki.publication.publication_object_elt.raise_if_error (*self*)

```
No-op, since this is not a <report_error/> PDU.
```

Definition at line 281 of file publication.py.

14.155.2.5 def rpki.publication.publication_object_elt.serve_dispatch (*self*, *r_msg*, *cb*, *eb*)

```
Action dispatch handler.
```

Definition at line 196 of file publication.py.

14.155.2.6 def rpki.publication.publication_object_elt.serve_publish (*self*)

```
Publish an object.
```

Definition at line 221 of file publication.py.

14.155.2.7 def rpki.publication.publication_object_elt.serve_withdraw (*self*)

```
Withdraw an object.
```

Definition at line 236 of file publication.py.

14.155.2.8 def rpki.publication.publication_object_elt.toXML (*self*)

```
Generate XML element for publishable object.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 187 of file publication.py.

14.155.2.9 def rpki.publication.publication_object_elt.uri_to_filename (*self*)

```
Convert a URI to a local filename.
```

Definition at line 250 of file publication.py.

14.155.3 Member Data Documentation

14.155.3.1 tuple rpki.publication.publication_object_elt.attributes = ("action", "tag", "client_handle", "uri") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 174 of file publication.py.

14.155.3.2 rpki.publication.publication_object_elt.payload = None [static]

Definition at line 176 of file publication.py.

14.155.3.3 rpki.publication.publication_object_elt.payload_type = None [static]

Reimplemented in rpki.publication.certificate_elt, rpki.publication.crl_elt, rpki.publication.manifest_elt, and rpki.publication.roa_elt.

Definition at line 175 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

14.156 rpki.publication.report_error_elt Class Reference

Inherits rpki::xml_utils::text_elt, and rpki::publication::publication_namespace.

Inherited by irbe_cli.report_error_elt.

Collaboration diagram for rpki.publication.report_error_elt:

Public Member Functions

- def __str__
- def from_exception
- def raise_if_error

Public Attributes

- error_code
- tag

Static Public Attributes

- tuple attributes = ("tag", "error_code")

  XML attributes for this element.

- string element_name = "report_error"
- error_text = None
- string text_attribute = "error_text"

  Name of the class attribute that holds the text value.

14.156.1 Detailed Description

```
<report_error/> element.
```

Definition at line 321 of file publication.py.

14.156.2 Member Function Documentation

14.156.2.1 def rpki.publication.report_error_elt.__str__ (*self*)

```
Convert a base_elt object to string format.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 343 of file publication.py.

14.156.2.2 def rpki.publication.report_error_elt.from_exception (*cls*, *e*, *tag* = None)

```
Generate a <report_error/> element from an exception.
```

Definition at line 333 of file publication.py.

14.156.2.3 def rpki.publication.report_error_elt.raise_if_error (*self*)

```
Raise exception associated with this <report_error/> PDU.
```

Definition at line 352 of file publication.py.

14.156.3 Member Data Documentation

14.156.3.1 tuple rpki.publication.report_error_elt.attributes = ("tag", "error_code") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 327 of file publication.py.

14.156.3.2 string rpki.publication.report_error_elt.element_name = "report_error" [static]

Definition at line 326 of file publication.py.

14.156.3.3 rpki.publication.report_error_elt.error_code

Definition at line 339 of file publication.py.

14.156.3.4 rpki.publication.report_error_elt.error_text = None [static]

Definition at line 330 of file publication.py.

14.156.3.5 rpki.publication.report_error_elt.tag

Definition at line 338 of file publication.py.

14.156.3.6 string rpki.publication.report_error_elt.text_attribute = "error_text" [static]

Name of the class attribute that holds the text value.

Reimplemented from rpki.xml_utils.text_elt.

Definition at line 328 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

14.157 rpki.publication.roa_elt Class Reference

Inherits rpki::publication::publication_object_elt.

Inherited by irbe_cli.roa_elt.

Collaboration diagram for rpki.publication.roa_elt:

Static Public Attributes

- string element_name = "roa"
- payload_type = rpki.x509.ROA

14.157.1 Detailed Description

`<roa/> element.`

Definition at line 311 of file publication.py.

14.157.2 Member Data Documentation

14.157.2.1 string rpki.publication.roa_elt.element_name = "roa" [static]

Definition at line 316 of file publication.py.

14.157.2.2 rpki.publication.roa_elt.payload_type = rpki.x509.ROA [static]

Reimplemented from rpki.publication.publication_object_elt.

Definition at line 317 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

14.158 rpki.publication.sax_handler Class Reference

Inherits rpki::xml_utils::sax_handler.

Inherited by irbe_cli.publication_sax_handler.

Collaboration diagram for rpki.publication.sax_handler:

Static Public Attributes

- string name = "msg"
- pdu = msg
- string version = "1"

14.158.1 Detailed Description

```
SAX handler for publication protocol.
```

Definition at line 406 of file publication.py.

14.158.2 Member Data Documentation

14.158.2.1 string rpki.publication.sax_handler.name = "msg" [static]

Definition at line 412 of file publication.py.

14.158.2.2 rpki.publication.sax_handler.pdu = msg [static]

Reimplemented in irbe_cli.publication_sax_handler.

Definition at line 411 of file publication.py.

14.158.2.3 string rpki.publication.sax_handler.version = "1" [static]

Definition at line 413 of file publication.py.

The documentation for this class was generated from the following file:

- publication.py (3107)

14.159 rpki.resource_set.resource_bag Class Reference

Inherits object.

Collaboration diagram for rpki.resource_set.resource_bag:

Public Member Functions

- def __eq__
- def __init__
- def __ne__
- def __str__
- def empty
- def from_rfc3779_tuples
- def intersection

- def oversized
- def undersized
- def union

Public Attributes

- asn

  Set of Autonomous System Number resources.

- v4

  Set of IPv4 resources.

- v6

  Set of IPv6 resources.

- valid_until

  Expiration date of resources, for setting certificate notAfter field.

14.159.1 Detailed Description

```
Container to simplify passing around the usual triple of ASN, IPv4,
and IPv6 resource sets.
```

Definition at line 547 of file resource_set.py.

14.159.2 Member Function Documentation

14.159.2.1 def rpki.resource_set.resource_bag.__eq__ (*self*, *other*)

Definition at line 615 of file resource_set.py.

14.159.2.2 def rpki.resource_set.resource_bag.__init__ (*self*, *asn* = `None`, *v4* = `None`, *v6* = `None`, *valid_until* = `None`)

Definition at line 565 of file resource_set.py.

14.159.2.3 def rpki.resource_set.resource_bag.__ne__ (*self*, *other*)

Definition at line 621 of file resource_set.py.

14.159.2.4 def rpki.resource_set.resource_bag.__str__ (*self*)

Definition at line 644 of file resource_set.py.

14.159.2.5 def rpki.resource_set.resource_bag.empty (*self*)

```
True iff all resource sets in this bag are empty.
```

Definition at line 611 of file resource_set.py.

14.159.2.6 def rpki.resource_set.resource_bag.from_rfc3779_tuples (*cls*, *exts*)

```
Build a resource_bag from intermediate form generated by RFC 3779
ASN.1 decoder.
```

Definition at line 588 of file resource_set.py.

14.159.2.7 def rpki.resource_set.resource_bag.intersection (*self*, *other*)

```
Compute intersection with another resource_bag.  valid_until
attribute (if any) inherits from self.
```

Definition at line 624 of file resource_set.py.

14.159.2.8 def rpki.resource_set.resource_bag.oversized (*self*, *other*)

```
True iff self is oversized with respect to other.
```

Definition at line 571 of file resource_set.py.

14.159.2.9 def rpki.resource_set.resource_bag.undersized (*self*, *other*)

```
True iff self is undersized with respect to other.
```

Definition at line 579 of file resource_set.py.

14.159.2.10 def rpki.resource_set.resource_bag.union (*self*, *other*)

```
Compute union with another resource_bag.  valid_until attribute
(if any) inherits from self.
```

Definition at line 634 of file resource_set.py.

14.159.3 Member Data Documentation

14.159.3.1 rpki::resource_set.resource_bag::asn

Set of Autonomous System Number resources.

Definition at line 566 of file resource_set.py.

14.159.3.2 rpki::resource_set.resource_bag::v4

Set of IPv4 resources.

Definition at line 567 of file resource_set.py.

14.159.3.3 rpki::resource_set.resource_bag::v6

Set of IPv6 resources.

Definition at line 568 of file resource_set.py.

14.159.3.4 rpki::resource_set.resource_bag::valid_until

Expiration date of resources, for setting certificate notAfter field.

Definition at line 569 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.160 rpki.resource_set.resource_range Class Reference

Inherits object.

Inherited by rpki.resource_set.resource_range_as, and rpki.resource_set.resource_-range_ip.

Collaboration diagram for rpki.resource_set.resource_range:

Public Member Functions

- def __cmp__
- def __init__

Public Attributes

- max

- min

14.160.1 Detailed Description

```
Generic resource range type.  Assumes underlying type is some kind
of integer.

This is a virtual class.  You probably don't want to use this type
directly.
```

Definition at line 50 of file resource_set.py.

14.160.2 Member Function Documentation

14.160.2.1 def rpki.resource_set.resource_range.__cmp__ (*self*, *other*)

```
Compare two resource_range objects.
```

Definition at line 67 of file resource_set.py.

14.160.2.2 def rpki.resource_set.resource_range.__init__ (*self*, *min*, *max*)

```
Initialize and sanity check a resource_range.
```

Definition at line 59 of file resource_set.py.

14.160.3 Member Data Documentation

14.160.3.1 rpki.resource_set.resource_range.max

Definition at line 65 of file resource_set.py.

14.160.3.2 rpki.resource_set.resource_range.min

Reimplemented in rpki.resource_set.resource_range_as.

Definition at line 64 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.161 rpki.resource_set.resource_range_as Class Reference

Inherits rpki::resource_set::resource_range.

Collaboration diagram for rpki.resource_set.resource_range_as:

Public Member Functions

- def __str__
- def to_rfc3779_tuple

Public Attributes

- min

Static Public Attributes

- datum_type = long

  Type of underlying data (min and max).

14.161.1 Detailed Description

```
Range of Autonomous System Numbers.

Denotes a single ASN by a range whose min and max values are
identical.
```

Definition at line 78 of file resource_set.py.

14.161.2 Member Function Documentation

14.161.2.1 def rpki.resource_set.resource_range_as.__str__ (*self*)

```
Convert a resource_range_as to string format.
```

Definition at line 91 of file resource_set.py.

14.161.2.2 def rpki.resource_set.resource_range_as.to_rfc3779_tuple (*self*)

```
Convert a resource_range_as to tuple format for RFC 3779 ASN.1 encoding.
```

Definition at line 100 of file resource_set.py.

14.161.3 Member Data Documentation

14.161.3.1 rpki::resource_set.resource_range_as::datum_type = long [static]

Type of underlying data (min and max).

Definition at line 89 of file resource_set.py.

14.161.3.2 rpki.resource_set.resource_range_as.min

Reimplemented from rpki.resource_set.resource_range.

Definition at line 95 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.162 rpki.resource_set.resource_range_ip Class Reference

Inherits rpki::resource_set::resource_range.

Inherited by rpki.resource_set.resource_range_ipv4, and rpki.resource_set.resource_-range_ipv6.

Collaboration diagram for rpki.resource_set.resource_range_ip:

Public Member Functions

- def __str__
- def make_prefix
- def to_rfc3779_tuple

Private Member Functions

- def _prefixlen

14.162.1 Detailed Description

```
Range of (generic) IP addresses.

Prefixes are converted to ranges on input, and ranges that can be
represented as prefixes are written as prefixes on output.

This is a virtual class.  You probably don't want to use it
directly.
```

Definition at line 109 of file resource_set.py.

14.162.2 Member Function Documentation

14.162.2.1 def rpki.resource_set.resource_range_ip.__str__ (*self*)

```
Convert a resource_range_ip to string format.
```

Definition at line 137 of file resource_set.py.

14.162.2.2 def rpki.resource_set.resource_range_ip._prefixlen (*self*) [private]

```
Determine whether a resource_range_ip can be expressed as a
prefix.
```

Definition at line 120 of file resource_set.py.

14.162.2.3 def rpki.resource_set.resource_range_ip.make_prefix (*cls*, *prefix*, *prefixlen*)

```
Construct a resource range corresponding to a prefix.
```

Definition at line 160 of file resource_set.py.

14.162.2.4 def rpki.resource_set.resource_range_ip.to_rfc3779_tuple (*self*)

```
Convert a resource_range_ip to tuple format for RFC 3779 ASN.1
encoding.
```

Definition at line 147 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.163 rpki.resource_set.resource_range_ipv4 Class Reference

Inherits rpki::resource_set::resource_range_ip.

Collaboration diagram for rpki.resource_set.resource_range_ipv4:

Static Public Attributes

- datum_type = rpki.ipaddrs.v4addr

  Type of underlying data (min and max).

14.163.1 Detailed Description

```
Range of IPv4 addresses.
```

Definition at line 170 of file resource_set.py.

14.163.2 Member Data Documentation

14.163.2.1 rpki::resource_set.resource_range_ipv4::datum_type = rpki.ipaddrs.v4addr [static]

Type of underlying data (min and max).

Definition at line 178 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.164 rpki.resource_set.resource_range_ipv6 Class Reference

Inherits rpki::resource_set::resource_range_ip.

Collaboration diagram for rpki.resource_set.resource_range_ipv6:

Static Public Attributes

- datum_type = rpki.ipaddrs.v6addr

  Type of underlying data (min and max).

14.164.1 Detailed Description

```
Range of IPv6 addresses.
```

Definition at line 180 of file resource_set.py.

14.164.2 Member Data Documentation

14.164.2.1 rpki::resource_set.resource_range_ipv6::datum_type = rpki.ipaddrs.v6addr [static]

Type of underlying data (min and max).

Definition at line 188 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.165 rpki.resource_set.resource_set Class Reference

Inherits list.

Inherited by rpki.resource_set.resource_set_as, and rpki.resource_set.resource_set_ip.

Collaboration diagram for rpki.resource_set.resource_set:

Public Member Functions

- def __init__
- def __str__
- def contains
- def difference
- def from_sql
- def intersection
- def issubset
- def issuperset
- def symmetric_difference
- def union

Static Public Attributes

- inherit = False

  Boolean indicating whether this resource_set uses RFC 3779 inheritance.

Private Member Functions

- def _comm

14.165.1 Detailed Description

```
Generic resource set, a list subclass containing resource ranges.

This is a virtual class.  You probably don't want to use it
directly.
```

Definition at line 206 of file resource_set.py.

14.165.2 Member Function Documentation

14.165.2.1 def rpki.resource_set.resource_set.__init__ (*self*, *ini* = `None`)

```
Initialize a resource_set.
```

Definition at line 219 of file resource_set.py.

14.165.2.2 def rpki.resource_set.resource_set.__str__ (*self*)

```
Convert a resource_set to string format.
```

Definition at line 246 of file resource_set.py.

14.165.2.3 def rpki.resource_set.resource_set._comm (*self*, *other*) [private]

```
Like comm(1), sort of.

Returns a tuple of three resource sets: resources only in self,
resources only in other, and resources in both.  Used (not very
efficiently) as the basis for most set operations on resource
sets.
```

Definition at line 255 of file resource_set.py.

14.165.2.4 def rpki.resource_set.resource_set.contains (*self*, *item*)

```
Set membership test for resource sets.
```

Definition at line 332 of file resource_set.py.

14.165.2.5 def rpki.resource_set.resource_set.difference (*self*, *other*)

```
Set difference for resource sets.
```

Definition at line 323 of file resource_set.py.

14.165.2.6 def rpki.resource_set.resource_set.from_sql (*cls*, *sql*, *query*, *args* = **None**)

```
Create resource set from an SQL query.

sql is an object that supports execute() and fetchall() methods
like a DB API 2.0 cursor object.

query is an SQL query that returns a sequence of (min, max) pairs.
```

Definition at line 369 of file resource_set.py.

14.165.2.7 def rpki.resource_set.resource_set.intersection (*self*, *other*)

```
Set intersection for resource sets.
```

Definition at line 319 of file resource_set.py.

14.165.2.8 def rpki.resource_set.resource_set.issubset (*self*, *other*)

```
Test whether self is a subset (possibly improper) of other.
```

Definition at line 355 of file resource_set.py.

14.165.2.9 def rpki.resource_set.resource_set.issuperset (*self*, *other*)

```
Test whether self is a superset (possibly improper) of other.
```

Definition at line 364 of file resource_set.py.

14.165.2.10 def rpki.resource_set.resource_set.symmetric_difference (*self*, *other*)

```
Set symmetric difference (XOR) for resource sets.
```

Definition at line 327 of file resource_set.py.

14.165.2.11 def rpki.resource_set.resource_set.union (*self*, *other*)

```
Set union for resource sets.
```

Definition at line 288 of file resource_set.py.

14.165.3 Member Data Documentation

14.165.3.1 rpki::resource_set.resource_set::inherit = False [static]

Boolean indicating whether this resource_set uses RFC 3779 inheritance.

Reimplemented in rpki.resource_set.resource_set_as, and rpki.resource_set.resource_set_ip.

Definition at line 217 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.166 rpki.resource_set.resource_set_as Class Reference

Inherits rpki::resource_set::resource_set.

Collaboration diagram for rpki.resource_set.resource_set_as:

Public Member Functions

- def parse_rfc3779_tuple
- def parse_str
- def to_rfc3779_tuple

Public Attributes

- inherit

  Boolean indicating whether this resource_set uses RFC 3779 inheritance.

Static Public Attributes

- range_type = resource_range_as

  Type of range underlying this type of resource_set.

14.166.1 Detailed Description

```
Autonomous System Number resource set.
```

Definition at line 384 of file resource_set.py.

14.166.2 Member Function Documentation

14.166.2.1 def rpki.resource_set.resource_set_as.parse_rfc3779_tuple (*self*, *x*)

```
Parse ASN resource from tuple format generated by RFC 3779 ASN.1
decoder.
```

Definition at line 404 of file resource_set.py.

14.166.2.2 def rpki.resource_set.resource_set_as.parse_str (*self*, *x*)

```
Parse ASN resource sets from text (eg, XML attributes).
```

Definition at line 394 of file resource_set.py.

14.166.2.3 def rpki.resource_set.resource_set_as.to_rfc3779_tuple (*self*)

```
Convert ASN resource set into tuple format used for RFC 3779 ASN.1
encoding.
```

Definition at line 422 of file resource_set.py.

14.166.3 Member Data Documentation

14.166.3.1 rpki.resource_set.resource_set_as.inherit

Boolean indicating whether this resource_set uses RFC 3779 inheritance.

Reimplemented from rpki.resource_set.resource_set.

Definition at line 420 of file resource_set.py.

14.166.3.2 rpki::resource_set.resource_set_as::range_type = resource_range_as [static]

Type of range underlying this type of resource_set.

Definition at line 392 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.167 rpki.resource_set.resource_set_ip Class Reference

Inherits rpki::resource_set::resource_set.

Inherited by rpki.resource_set.resource_set_ipv4, and rpki.resource_set.resource_set_-ipv6.

Collaboration diagram for rpki.resource_set.resource_set_ip:

Public Member Functions

- def parse_rfc3779_tuple
- def parse_str
- def to_rfc3779_tuple

Public Attributes

- inherit

  Boolean indicating whether this resource_set uses RFC 3779 inheritance.

14.167.1 Detailed Description

```
(Generic) IP address resource set.

This is a virtual class.  You probably don't want to use it
directly.
```

Definition at line 434 of file resource_set.py.

14.167.2 Member Function Documentation

14.167.2.1 def rpki.resource_set.resource_set_ip.parse_rfc3779_tuple (*self*, *x*)

```
Parse IP address resource sets from tuple format generated by RFC
3779 ASN.1 decoder.
```

Definition at line 454 of file resource_set.py.

14.167.2.2 def rpki.resource_set.resource_set_ip.parse_str (*self*, *x*)

```
Parse IP address resource sets from text (eg, XML attributes).
```

Definition at line 442 of file resource_set.py.

14.167.2.3 def rpki.resource_set.resource_set_ip.to_rfc3779_tuple (*self*)

```
Convert IP resource set into tuple format used by RFC 3779 ASN.1
encoder.
```

Definition at line 472 of file resource_set.py.

14.167.3 Member Data Documentation

14.167.3.1 rpki.resource_set.resource_set_ip.inherit

Boolean indicating whether this resource_set uses RFC 3779 inheritance.

Reimplemented from rpki.resource_set.resource_set.

Definition at line 470 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.168 rpki.resource_set.resource_set_ipv4 Class Reference

Inherits rpki::resource_set::resource_set_ip.

Collaboration diagram for rpki.resource_set.resource_set_ipv4:

Static Public Attributes

- string afi = "\x00\x01"

  Address Family Identifier value for IPv4.

- range_type = resource_range_ipv4

  Type of range underlying this type of resource_set.

14.168.1 Detailed Description

```
IPv4 address resource set.
```

Definition at line 484 of file resource_set.py.

14.168.2 Member Data Documentation

14.168.2.1 rpki::resource_set.resource_set_ipv4::afi = "\x00\x01" [static]

Address Family Identifier value for IPv4.

Definition at line 497 of file resource_set.py.

14.168.2.2 rpki::resource_set.resource_set_ipv4::range_type = resource_range_ipv4 [static]

Type of range underlying this type of resource_set.

Definition at line 492 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.169 rpki.resource_set.resource_set_ipv6 Class Reference

Inherits rpki::resource_set::resource_set_ip.

Collaboration diagram for rpki.resource_set.resource_set_ipv6:

Static Public Attributes

- string afi = "\x00\x02"

  Address Family Identifier value for IPv6.

- range_type = resource_range_ipv6

  Type of range underlying this type of resource_set.

14.169.1 Detailed Description

```
IPv6 address resource set.
```

Definition at line 499 of file resource_set.py.

14.169.2 Member Data Documentation

14.169.2.1 rpki::resource_set.resource_set_ipv6::afi = "\x00\x02" [static]

Address Family Identifier value for IPv6.

Definition at line 512 of file resource_set.py.

14.169.2.2 rpki::resource_set.resource_set_ipv6::range_type = resource_range_ipv6 [static]

Type of range underlying this type of resource_set.

Definition at line 507 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.170 rpki.resource_set.roa_prefix Class Reference

Inherits object.

Inherited by rpki.resource_set.roa_prefix_ipv4, and rpki.resource_set.roa_prefix_ipv6.

Collaboration diagram for rpki.resource_set.roa_prefix:

Public Member Functions

- def __cmp__
- def __init__
- def __str__
- def max
- def min
- def to_resource_range
- def to_roa_tuple

Public Attributes

- max_prefixlen

Maxmimum prefix length.

- prefix

  The prefix itself, an IP address with bits beyond the prefix length zeroed.

- prefixlen

  (Minimum) prefix length.

14.170.1 Detailed Description

```
ROA prefix.  This is similar to the resource_range_ip class, but
differs in that it only represents prefixes, never ranges, and
includes the maximum prefix length as an additional value.

This is a virtual class, you probably don't want to use it directly.
```

Definition at line 666 of file resource_set.py.

14.170.2 Member Function Documentation

14.170.2.1 def rpki.resource_set.roa_prefix.__cmp__ (*self*, *other*)

```
Compare two ROA prefix objects.  Comparision is based on prefix,
prefixlen, and max_prefixlen, in that order.
```

Definition at line 697 of file resource_set.py.

14.170.2.2 def rpki.resource_set.roa_prefix.__init__ (*self*, *prefix*, *prefixlen*, *max_prefixlen* = `None`)

```
Initialize a ROA prefix.  max_prefixlen is optional and defaults
to prefixlen.  max_prefixlen must not be smaller than prefixlen.
```

Definition at line 685 of file resource_set.py.

14.170.2.3 def rpki.resource_set.roa_prefix.__str__ (*self*)

```
Convert a ROA prefix to string format.
```

Definition at line 710 of file resource_set.py.

14.170.2.4 def rpki.resource_set.roa_prefix.max (*self*)

```
Return highest address covered by prefix.
```

Definition at line 731 of file resource_set.py.

14.170.2.5 def rpki.resource_set.roa_prefix.min (*self*)

```
Return lowest address covered by prefix.
```

Definition at line 727 of file resource_set.py.

14.170.2.6 def rpki.resource_set.roa_prefix.to_resource_range (*self*)

```
Convert this ROA prefix to the equivilent resource_range_ip
object.  This is an irreversable transformation because it loses
the max_prefixlen attribute, nothing we can do about that.
```

Definition at line 719 of file resource_set.py.

14.170.2.7 def rpki.resource_set.roa_prefix.to_roa_tuple (*self*)

```
Convert a resource_range_ip to tuple format for ROA ASN.1
encoding.
```

Definition at line 738 of file resource_set.py.

14.170.3 Member Data Documentation

14.170.3.1 rpki::resource_set.roa_prefix::max_prefixlen

Maxmimum prefix length.

Definition at line 695 of file resource_set.py.

14.170.3.2 rpki::resource_set.roa_prefix::prefix

The prefix itself, an IP address with bits beyond the prefix length zeroed.

Definition at line 693 of file resource_set.py.

14.170.3.3 rpki::resource_set.roa_prefix::prefixlen

(Minimum) prefix length.

Definition at line 694 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.171 rpki.resource_set.roa_prefix_ipv4 Class Reference

Inherits rpki::resource_set::roa_prefix.

Collaboration diagram for rpki.resource_set.roa_prefix_ipv4:

Static Public Attributes

- range_type = resource_range_ipv4

  Type of corresponding resource_range_ip.

14.171.1 Detailed Description

```
IPv4 ROA prefix.
```

Definition at line 746 of file resource_set.py.

14.171.2 Member Data Documentation

14.171.2.1 rpki::resource_set.roa_prefix_ipv4::range_type = resource_range_ipv4 [static]

Type of corresponding resource_range_ip.

Definition at line 754 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.172 rpki.resource_set.roa_prefix_ipv6 Class Reference

Inherits rpki::resource_set::roa_prefix.

Collaboration diagram for rpki.resource_set.roa_prefix_ipv6:

Static Public Attributes

- range_type = resource_range_ipv6

  Type of corresponding resource_range_ip.

14.172.1 Detailed Description

```
IPv6 ROA prefix.
```

Definition at line 756 of file resource_set.py.

14.172.2 Member Data Documentation

14.172.2.1 rpki::resource_set.roa_prefix_ipv6::range_type = resource_range_ipv6 [static]

Type of corresponding resource_range_ip.

Definition at line 764 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.173 rpki.resource_set.roa_prefix_set Class Reference

Inherits list.

Inherited by rpki.resource_set.roa_prefix_set_ipv4, and rpki.resource_set.roa_prefix_-set_ipv6.

Collaboration diagram for rpki.resource_set.roa_prefix_set:

Public Member Functions

- def __init__
- def __str__
- def from_sql
- def parse_str
- def to_resource_set
- def to_roa_tuple

14.173.1 Detailed Description

```
Set of ROA prefixes, analogous to the resource_set_ip class.
```

Definition at line 766 of file resource_set.py.

14.173.2 Member Function Documentation

14.173.2.1 def rpki.resource_set.roa_prefix_set.__init__ (*self*, *ini* = `None`)

```
Initialize a ROA prefix set.
```

Definition at line 771 of file resource_set.py.

14.173.2.2 def rpki.resource_set.roa_prefix_set.__str__ (*self*)

```
Convert a ROA prefix set to string format.
```

Definition at line 791 of file resource_set.py.

14.173.2.3 def rpki.resource_set.roa_prefix_set.from_sql (*cls*, *sql*, *query*, *args* = `None`)

```
Create ROA prefix set from an SQL query.

sql is an object that supports execute() and fetchall() methods
like a DB API 2.0 cursor object.

query is an SQL query that returns a sequence of (prefix,
prefixlen, max_prefixlen) triples.
```

Definition at line 825 of file resource_set.py.

14.173.2.4 def rpki.resource_set.roa_prefix_set.parse_str (*self*, *x*)

```
Parse ROA prefix from text (eg, an XML attribute).
```

Definition at line 795 of file resource_set.py.

14.173.2.5 def rpki.resource_set.roa_prefix_set.to_resource_set (*self*)

```
Convert a ROA prefix set to a resource set.  This is an
irreversable transformation.  We have to compute a union here
because ROA prefix sets can include overlaps, while RFC 3779
resource sets cannot.  This is ugly, and there is almost certainly
a more efficient way to do this, but start by getting the output
right before worrying about making it fast or pretty.
```

Definition at line 807 of file resource_set.py.

14.173.2.6 def rpki.resource_set.roa_prefix_set.to_roa_tuple (*self*)

```
Convert ROA prefix set into tuple format used by ROA ASN.1
encoder.  This is a variation on the format used in RFC 3779.
```

Definition at line 840 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.174 rpki.resource_set.roa_prefix_set_ipv4 Class Reference

Inherits rpki::resource_set::roa_prefix_set.

Collaboration diagram for rpki.resource_set.roa_prefix_set_ipv4:

Static Public Attributes

- prefix_type = roa_prefix_ipv4

  Type of underlying roa_prefix.

- resource_set_type = resource_set_ipv4

  Type of corresponding resource_set_ip class.

14.174.1 Detailed Description

```
Set of IPv4 ROA prefixes.
```

Definition at line 850 of file resource_set.py.

14.174.2 Member Data Documentation

14.174.2.1 rpki::resource_set.roa_prefix_set_ipv4::prefix_type = roa_prefix_ipv4 [static]

Type of underlying roa_prefix.

Definition at line 858 of file resource_set.py.

14.174.2.2 rpki::resource_set.roa_prefix_set_ipv4::resource_set_type = resource_set_ipv4 [static]

Type of corresponding resource_set_ip class.

Definition at line 863 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.175 rpki.resource_set.roa_prefix_set_ipv6 Class Reference

Inherits rpki::resource_set::roa_prefix_set.

Collaboration diagram for rpki.resource_set.roa_prefix_set_ipv6:

Static Public Attributes

- prefix_type = roa_prefix_ipv6

  Type of underlying roa_prefix.

- resource_set_type = resource_set_ipv6

  Type of corresponding resource_set_ip class.

14.175.1 Detailed Description

```
Set of IPv6 ROA prefixes.
```

Definition at line 865 of file resource_set.py.

14.175.2 Member Data Documentation

14.175.2.1 rpki::resource_set.roa_prefix_set_ipv6::prefix_type = roa_prefix_ipv6 [static]

Type of underlying roa_prefix.

Definition at line 873 of file resource_set.py.

14.175.2.2 rpki::resource_set.roa_prefix_set_ipv6::resource_set_type = resource_set_ipv6 [static]

Type of corresponding resource_set_ip class.

Definition at line 878 of file resource_set.py.

The documentation for this class was generated from the following file:

- resource_set.py (3107)

14.176 rpki.roa.ROAIPAddress Class Reference

Inherits Sequence.

Collaboration diagram for rpki.roa.ROAIPAddress:

Public Member Functions

- def __init__

Public Attributes

- address
- maxLength

14.176.1 Detailed Description

Definition at line 47 of file roa.py.

14.176.2 Member Function Documentation

14.176.2.1 def rpki.roa.ROAIPAddress.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 48 of file roa.py.

14.176.3 Member Data Documentation

14.176.3.1 rpki.roa.ROAIPAddress.address

Definition at line 49 of file roa.py.

14.176.3.2 rpki.roa.ROAIPAddress.maxLength

Definition at line 50 of file roa.py.

The documentation for this class was generated from the following file:

- roa.py (2424)

14.177 rpki.roa.ROAIPAddresses Class Reference

Inherits SequenceOf.

Collaboration diagram for rpki.roa.ROAIPAddresses:

Public Member Functions

- def __init__

14.177.1 Detailed Description

Definition at line 54 of file roa.py.

14.177.2 Member Function Documentation

14.177.2.1 def rpki.roa.ROAIPAddresses.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 55 of file roa.py.

The documentation for this class was generated from the following file:

- roa.py (2424)

14.178 rpki.roa.ROAIPAddressFamilies Class Reference

Inherits SequenceOf.

Collaboration diagram for rpki.roa.ROAIPAddressFamilies:

Public Member Functions

- def __init__

14.178.1 Detailed Description

Definition at line 65 of file roa.py.

14.178.2 Member Function Documentation

14.178.2.1 def rpki.roa.ROAIPAddressFamilies.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 66 of file roa.py.

The documentation for this class was generated from the following file:

- roa.py (2424)

14.179 rpki.roa.ROAIPAddressFamily Class Reference

Inherits Sequence.

Collaboration diagram for rpki.roa.ROAIPAddressFamily:

Public Member Functions

- def __init__

Public Attributes

- addresses
- addressFamily

14.179.1 Detailed Description

Definition at line 58 of file roa.py.

14.179.2 Member Function Documentation

14.179.2.1 def rpki.roa.ROAIPAddressFamily.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 59 of file roa.py.

14.179.3 Member Data Documentation

14.179.3.1 rpki.roa.ROAIPAddressFamily.addresses

Definition at line 61 of file roa.py.

14.179.3.2 rpki.roa.ROAIPAddressFamily.addressFamily

Definition at line 60 of file roa.py.

The documentation for this class was generated from the following file:

- roa.py (2424)

14.180 rpki.roa.RouteOriginAttestation Class Reference

Inherits Sequence.

Collaboration diagram for rpki.roa.RouteOriginAttestation:

Public Member Functions

- def __init__

Public Attributes

- asID
- explicitVersion
- ipAddrBlocks
- version

14.180.1 Detailed Description

Definition at line 69 of file roa.py.

14.180.2 Member Function Documentation

14.180.2.1 def rpki.roa.RouteOriginAttestation.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 70 of file roa.py.

14.180.3 Member Data Documentation

14.180.3.1 rpki.roa.RouteOriginAttestation.asID

Definition at line 73 of file roa.py.

14.180.3.2 rpki.roa.RouteOriginAttestation.explicitVersion

Definition at line 72 of file roa.py.

14.180.3.3 rpki.roa.RouteOriginAttestation.ipAddrBlocks

Definition at line 74 of file roa.py.

14.180.3.4 rpki.roa.RouteOriginAttestation.version

Definition at line 71 of file roa.py.

The documentation for this class was generated from the following file:

- roa.py (2424)

14.181 rpki.rpki_engine.ca_detail_obj Class Reference

Inherits rpki::sql::sql_persistent.

Collaboration diagram for rpki.rpki_engine.ca_detail_obj:

Public Member Functions

- def activate
- def ca
- def child_certs
- def create
- def crl_published_callback

- def crl_uri
- def crl_uri_tail
- def delete
- def generate_crl
- def generate_manifest
- def generate_manifest_cert
- def issue
- def issue_ee
- def manifest_published_callback
- def manifest_uri
- def revoke
- def revoked_certs
- def roas
- def sql_decode
- def update

Public Attributes

- ca_cert_uri
- ca_id
- gctx
- latest_crl
- latest_manifest
- latest_manifest_cert
- manifest_private_key_id
- manifest_public_key
- nextUpdate
- private_key_id
- public_key
- state

Static Public Attributes

- crl_published = None
- latest_ca_cert = None
- manifest_published = None
- tuple sql_template

14.181.1 Detailed Description

```
Internal CA detail object.
```

Definition at line 562 of file rpki_engine.py.

14.181.2 Member Function Documentation

14.181.2.1 def rpki.rpki_engine.ca_detail_obj.activate (*self*, *ca*, *cert*, *uri*, *callback*, *errback*, *predecessor* = `None`)

```
Activate this ca_detail.
```

Definition at line 624 of file rpki_engine.py.

14.181.2.2 def rpki.rpki_engine.ca_detail_obj.ca (*self*)

```
Fetch CA object to which this ca_detail links.
```

Definition at line 596 of file rpki_engine.py.

14.181.2.3 def rpki.rpki_engine.ca_detail_obj.child_certs (*self*, *child* = `None`, *ski* = `None`, *unique* = `False`)

```
Fetch all child_cert objects that link to this ca_detail.
```

Definition at line 600 of file rpki_engine.py.

14.181.2.4 def rpki.rpki_engine.ca_detail_obj.create (*cls*, *ca*)

```
Create a new ca_detail object for a specified CA.
```

Definition at line 762 of file rpki_engine.py.

14.181.2.5 def rpki.rpki_engine.ca_detail_obj.crl_published_callback (*self*, *pdu*)

```
Check result of CRL publication.
```

Definition at line 885 of file rpki_engine.py.

14.181.2.6 def rpki.rpki_engine.ca_detail_obj.crl_uri (*self*, *ca*)

```
Return publication URI for this ca_detail's CRL.
```

Definition at line 612 of file rpki_engine.py.

14.181.2.7 def rpki.rpki_engine.ca_detail_obj.crl_uri_tail (*self*)

```
Return tail (filename portion) of publication URI for this ca_detail's CRL.
```

Definition at line 616 of file rpki_engine.py.

14.181.2.8 def rpki.rpki_engine.ca_detail_obj.delete (*self*, *ca*, *publisher*, *allow_failure* = `False`)

```
Delete this ca_detail and all of the certs it issued.

If allow_failure is true, we clean up as much as we can but don't
raise an exception.
```

Definition at line 649 of file rpki_engine.py.

14.181.2.9 def rpki.rpki_engine.ca_detail_obj.generate_crl (*self*, *publisher*, *nextUpdate* = `None`)

```
Generate a new CRL for this ca_detail.  At the moment this is
unconditional, that is, it is up to the caller to decide whether a
new CRL is needed.
```

Definition at line 849 of file rpki_engine.py.

14.181.2.10 def rpki.rpki_engine.ca_detail_obj.generate_manifest (*self*, *publisher*, *nextUpdate* = `None`)

```
Generate a new manifest for this ca_detail.
```

Definition at line 893 of file rpki_engine.py.

14.181.2.11 def rpki.rpki_engine.ca_detail_obj.generate_manifest_cert (*self*, *ca*)

```
Generate a new manifest certificate for this ca_detail.
```

Definition at line 797 of file rpki_engine.py.

14.181.2.12 def rpki.rpki_engine.ca_detail_obj.issue (*self*, *ca*, *child*, *subject_key*, *sia*, *resources*, *publisher*, *child_cert* = None)

```
Issue a new certificate to a child.  Optional child_cert argument
specifies an existing child_cert object to update in place; if not
specified, we create a new one.  Returns the child_cert object
containing the newly issued cert.
```

Definition at line 809 of file rpki_engine.py.

14.181.2.13 def rpki.rpki_engine.ca_detail_obj.issue_ee (*self*, *ca*, *resources*, *subject_key*, *sia* = None)

```
Issue a new EE certificate.
```

Definition at line 780 of file rpki_engine.py.

14.181.2.14 def rpki.rpki_engine.ca_detail_obj.manifest_published_callback (*self*, *pdu*)

```
Check result of manifest publication.
```

Definition at line 927 of file rpki_engine.py.

14.181.2.15 def rpki.rpki_engine.ca_detail_obj.manifest_uri (*self*, *ca*)

```
Return publication URI for this ca_detail's manifest.
```

Definition at line 620 of file rpki_engine.py.

14.181.2.16 def rpki.rpki_engine.ca_detail_obj.revoke (*self*, *cb*, *eb*)

```
Request revocation of all certificates whose SKI matches the key
for this ca_detail.

Tasks:

- Request revocation of old keypair by parent.

- Revoke all child certs issued by the old keypair.

- Generate a final CRL, signed with the old keypair, listing all
  the revoked certs, with a next CRL time after the last cert or
  CRL signed by the old keypair will have expired.

- Generate a corresponding final manifest.

- Destroy old keypairs.

- Leave final CRL and manifest in place until their nextupdate
  time has passed.
```

Definition at line 673 of file rpki_engine.py.

14.181.2.17 def rpki.rpki_engine.ca_detail_obj.revoked_certs (*self*)

```
Fetch all revoked_cert objects that link to this ca_detail.
```

Definition at line 604 of file rpki_engine.py.

14.181.2.18 def rpki.rpki_engine.ca_detail_obj.roas (*self*)

```
Fetch all ROA objects that link to this ca_detail.
```

Definition at line 608 of file rpki_engine.py.

14.181.2.19 def rpki.rpki_engine.ca_detail_obj.sql_decode (*self*, *vals*)

```
Extra assertions for SQL decode of a ca_detail_obj.
```

Reimplemented from rpki.sql.sql_persistent.

Definition at line 588 of file rpki_engine.py.

14.181.2.20 def rpki.rpki_engine.ca_detail_obj.update (*self*, *parent*, *ca*, *rc*, *sia_uri_changed*, *old_resources*, *callback*, *errback*)

```
Need to get a new certificate for this ca_detail and perhaps frob
children of this ca_detail.
```

Definition at line 737 of file rpki_engine.py.

14.181.3 Member Data Documentation

14.181.3.1 rpki.rpki_engine.ca_detail_obj.ca_cert_uri

Definition at line 632 of file rpki_engine.py.

14.181.3.2 rpki.rpki_engine.ca_detail_obj.ca_id

Definition at line 768 of file rpki_engine.py.

14.181.3.3 rpki.rpki_engine.ca_detail_obj.crl_published = None [static]

Definition at line 584 of file rpki_engine.py.

14.181.3.4 rpki.rpki_engine.ca_detail_obj.gctx

Reimplemented from rpki.sql.sql_persistent.

Definition at line 767 of file rpki_engine.py.

14.181.3.5 rpki.rpki_engine.ca_detail_obj.latest_ca_cert = None [static]

Definition at line 586 of file rpki_engine.py.

14.181.3.6 rpki.rpki_engine.ca_detail_obj.latest_crl

Definition at line 872 of file rpki_engine.py.

14.181.3.7 rpki.rpki_engine.ca_detail_obj.latest_manifest

Definition at line 913 of file rpki_engine.py.

14.181.3.8 rpki.rpki_engine.ca_detail_obj.latest_manifest_cert

Definition at line 730 of file rpki_engine.py.

14.181.3.9 rpki.rpki_engine.ca_detail_obj.manifest_private_key_id

Definition at line 728 of file rpki_engine.py.

14.181.3.10 rpki.rpki_engine.ca_detail_obj.manifest_public_key

Definition at line 729 of file rpki_engine.py.

14.181.3.11 rpki.rpki_engine.ca_detail_obj.manifest_published = None [static]

Definition at line 585 of file rpki_engine.py.

14.181.3.12 rpki.rpki_engine.ca_detail_obj.nextUpdate

Definition at line 706 of file rpki_engine.py.

14.181.3.13 rpki.rpki_engine.ca_detail_obj.private_key_id

Definition at line 727 of file rpki_engine.py.

14.181.3.14 rpki.rpki_engine.ca_detail_obj.public_key

Definition at line 772 of file rpki_engine.py.

14.181.3.15 tuple rpki.rpki_engine.ca_detail_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
    "ca_detail",
    "ca_detail_id",
    ("private_key_id",          rpki.x509.RSA),
    ("public_key",              rpki.x509.RSApublic),
    ("latest_ca_cert",          rpki.x509.X509),
    ("manifest_private_key_id", rpki.x509.RSA),
    ("manifest_public_key",     rpki.x509.RSApublic),
    ("latest_manifest_cert",    rpki.x509.X509),
    ("latest_manifest",         rpki.x509.SignedManifest),
    ("latest_crl",              rpki.x509.CRL),
    ("crl_published",           rpki.sundial.datetime),
    ("manifest_published",      rpki.sundial.datetime),
    "state",
    "ca_cert_uri",
    "ca_id")
```

Definition at line 567 of file rpki_engine.py.

14.181.3.16 rpki.rpki_engine.ca_detail_obj.state

Definition at line 634 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- rpki_engine.py (3107)

14.182 rpki.rpki_engine.ca_obj Class Reference

Inherits rpki::sql::sql_persistent.

Collaboration diagram for rpki.rpki_engine.ca_obj:

Public Member Functions

- def ca_details
- def check_for_updates
- def construct_sia_uri
- def create
- def delete

- def fetch_active
- def fetch_deprecated
- def fetch_issue_response_candidates
- def fetch_pending
- def fetch_revoked
- def next_crl_number
- def next_manifest_number
- def next_serial_number
- def parent
- def rekey
- def revoke

Public Attributes

- gctx
- parent_id
- parent_resource_class
- sia_uri

Static Public Attributes

- int last_crl_sn = 0
- int last_issued_sn = 0
- int last_manifest_sn = 0
- tuple sql_template

14.182.1 Detailed Description

```
Internal CA object.
```

Definition at line 308 of file rpki_engine.py.

14.182.2 Member Function Documentation

14.182.2.1 def rpki.rpki_engine.ca_obj.ca_details (*self*)

```
Fetch all ca_detail objects that link to this CA object.
```

Definition at line 330 of file rpki_engine.py.

14.182.2.2 def rpki.rpki_engine.ca_obj.check_for_updates (*self*, *parent*, *rc*, *cb*, *eb*)

```
Parent has signaled continued existance of a resource class we
already knew about, so we need to check for an updated
certificate, changes in resource coverage, revocation and reissue
with the same key, etc.
```

Definition at line 371 of file rpki_engine.py.

14.182.2.3 def rpki.rpki_engine.ca_obj.construct_sia_uri (*self*, *parent*, *rc*)

```
Construct the sia_uri value for this CA given configured
information and the parent's up-down protocol list_response PDU.
```

Definition at line 358 of file rpki_engine.py.

14.182.2.4 def rpki.rpki_engine.ca_obj.create (*cls*, *parent*, *rc*, *cb*, *eb*)

```
Parent has signaled existance of a new resource class, so we need
to create and set up a corresponding CA object.
```

Definition at line 451 of file rpki_engine.py.

14.182.2.5 def rpki.rpki_engine.ca_obj.delete (*self*, *parent*, *callback*)

```
The list of current resource classes received from parent does not
include the class corresponding to this CA, so we need to delete
it (and its little dog too...).

All certs published by this CA are now invalid, so need to
withdraw them, the CRL, and the manifest from the repository,
delete all child_cert and ca_detail records associated with this
CA, then finally delete this CA itself.
```

Definition at line 475 of file rpki_engine.py.

14.182.2.6 def rpki.rpki_engine.ca_obj.fetch_active (*self*)

```
Fetch the active ca_detail for this CA, if any.
```

Definition at line 338 of file rpki_engine.py.

14.182.2.7 def rpki.rpki_engine.ca_obj.fetch_deprecated (*self*)

```
Fetch deprecated ca_details for this CA, if any.
```

Definition at line 342 of file rpki_engine.py.

14.182.2.8 def rpki.rpki_engine.ca_obj.fetch_issue_response_candidates (*self*)

```
Fetch ca_details which are candidates for consideration when
processing an up-down issue_response PDU.
```

Definition at line 350 of file rpki_engine.py.

14.182.2.9 def rpki.rpki_engine.ca_obj.fetch_pending (*self*)

```
Fetch the pending ca_details for this CA, if any.
```

Definition at line 334 of file rpki_engine.py.

14.182.2.10 def rpki.rpki_engine.ca_obj.fetch_revoked (*self*)

```
Fetch revoked ca_details for this CA, if any.
```

Definition at line 346 of file rpki_engine.py.

14.182.2.11 def rpki.rpki_engine.ca_obj.next_crl_number (*self*)

```
Allocate a CRL serial number.
```

Definition at line 517 of file rpki_engine.py.

14.182.2.12 def rpki.rpki_engine.ca_obj.next_manifest_number (*self*)

```
Allocate a manifest serial number.
```

Definition at line 509 of file rpki_engine.py.

14.182.2.13 def rpki.rpki_engine.ca_obj.next_serial_number (*self*)

```
Allocate a certificate serial number.
```

Definition at line 501 of file rpki_engine.py.

14.182.2.14 def rpki.rpki_engine.ca_obj.parent (*self*)

```
Fetch parent object to which this CA object links.
```

Definition at line 326 of file rpki_engine.py.

14.182.2.15 def rpki.rpki_engine.ca_obj.rekey (*self*, *cb*, *eb*)

```
Initiate a rekey operation for this ca.  Generate a new keypair.
Request cert from parent using new keypair.  Mark result as our
active ca_detail.  Reissue all child certs issued by this ca using
the new ca_detail.
```

Definition at line 525 of file rpki_engine.py.

14.182.2.16 def rpki.rpki_engine.ca_obj.revoke (*self*, *cb*, *eb*)

```
Revoke deprecated ca_detail objects associated with this ca.
```

Definition at line 550 of file rpki_engine.py.

14.182.3 Member Data Documentation

14.182.3.1 rpki.rpki_engine.ca_obj.gctx

Reimplemented from rpki.sql.sql_persistent.

Definition at line 458 of file rpki_engine.py.

14.182.3.2 int rpki.rpki_engine.ca_obj.last_crl_sn = 0 [static]

Definition at line 322 of file rpki_engine.py.

14.182.3.3 int rpki.rpki_engine.ca_obj.last_issued_sn = 0 [static]

Definition at line 323 of file rpki_engine.py.

14.182.3.4 int rpki.rpki_engine.ca_obj.last_manifest_sn = 0 [static]

Definition at line 324 of file rpki_engine.py.

14.182.3.5 rpki.rpki_engine.ca_obj.parent_id

Definition at line 459 of file rpki_engine.py.

14.182.3.6 rpki.rpki_engine.ca_obj.parent_resource_class

Definition at line 460 of file rpki_engine.py.

14.182.3.7 rpki.rpki_engine.ca_obj.sia_uri

Definition at line 382 of file rpki_engine.py.

14.182.3.8 tuple rpki.rpki_engine.ca_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
    "ca",
    "ca_id",
    "last_crl_sn",
    ("next_crl_update", rpki.sundial.datetime),
    "last_issued_sn", "last_manifest_sn",
    ("next_manifest_update", rpki.sundial.datetime),
    "sia_uri", "parent_id", "parent_resource_class")
```

Definition at line 313 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- rpki_engine.py (3107)

14.183 rpki.rpki_engine.child_cert_obj Class Reference

Inherits rpki::sql::sql_persistent.

Collaboration diagram for rpki.rpki_engine.child_cert_obj:

Public Member Functions

- def __init__
- def ca_detail
- def child
- def fetch
- def published_callback

- def reissue
- def revoke
- def uri
- def uri_tail

Public Attributes

- ca_detail_id
- cert
- child_id
- gctx
- published

Static Public Attributes

- tuple sql_template

14.183.1 Detailed Description

```
Certificate that has been issued to a child.
```

Definition at line 936 of file rpki_engine.py.

14.183.2 Member Function Documentation

14.183.2.1 def rpki.rpki_engine.child_cert_obj.__init__ (*self*, *gctx* = `None`, *child_id* = `None`, *ca_detail_id* = `None`, *cert* = `None`)

```
Initialize a child_cert_obj.
```

Definition at line 950 of file rpki_engine.py.

14.183.2.2 def rpki.rpki_engine.child_cert_obj.ca_detail (*self*)

```
Fetch ca_detail object to which this child_cert object links.
```

Definition at line 967 of file rpki_engine.py.

14.183.2.3 def rpki.rpki_engine.child_cert_obj.child (*self*)

```
Fetch child object to which this child_cert object links.
```

Definition at line 963 of file rpki_engine.py.

14.183.2.4 def rpki.rpki_engine.child_cert_obj.fetch (*cls*, *gctx* = **None**, *child* = **None**, *ca_detail* = **None**, *ski* = **None**, *unique* = **False**)

```
Fetch all child_cert objects matching a particular set of
parameters.  This is a wrapper to consolidate various queries that
would otherwise be inline SQL WHERE expressions.  In most cases
code calls this indirectly, through methods in other classes.
```

Definition at line 1048 of file rpki_engine.py.

14.183.2.5 def rpki.rpki_engine.child_cert_obj.published_callback (*self*, *pdu*)

```
Publication callback: check result and mark published.
```

Definition at line 1080 of file rpki_engine.py.

14.183.2.6 def rpki.rpki_engine.child_cert_obj.reissue (*self*, *ca_detail*, *publisher*, *resources* = **None**, *sia* = **None**)

```
Reissue an existing child cert, reusing the public key.  If the
child cert we would generate is identical to the one we already
have, we just return the one we already have.  If we have to
revoke the old child cert when generating the new one, we have to
generate a new child_cert_obj, so calling code that needs the
updated child_cert_obj must use the return value from this method.
```

Definition at line 991 of file rpki_engine.py.

14.183.2.7 def rpki.rpki_engine.child_cert_obj.revoke (*self*, *publisher*)

```
Revoke a child cert.
```

Definition at line 979 of file rpki_engine.py.

14.183.2.8 def rpki.rpki_engine.child_cert_obj.uri (*self*, *ca*)

```
Return the publication URI for this child_cert.
```

Definition at line 975 of file rpki_engine.py.

14.183.2.9 def rpki.rpki_engine.child_cert_obj.uri_tail (*self*)

```
Return the tail (filename) portion of the URI for this child_cert.
```

Definition at line 971 of file rpki_engine.py.

14.183.3 Member Data Documentation

14.183.3.1 rpki.rpki_engine.child_cert_obj.ca_detail_id

Definition at line 957 of file rpki_engine.py.

14.183.3.2 rpki.rpki_engine.child_cert_obj.cert

Definition at line 958 of file rpki_engine.py.

14.183.3.3 rpki.rpki_engine.child_cert_obj.child_id

Definition at line 956 of file rpki_engine.py.

14.183.3.4 rpki.rpki_engine.child_cert_obj.gctx

Reimplemented from rpki.sql.sql_persistent.

Definition at line 955 of file rpki_engine.py.

14.183.3.5 rpki.rpki_engine.child_cert_obj.published

Definition at line 959 of file rpki_engine.py.

14.183.3.6 tuple rpki.rpki_engine.child_cert_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
    "child_cert",
    "child_cert_id",
    ("cert", rpki.x509.X509),
    "child_id",
    "ca_detail_id",
    "ski",
    ("published", rpki.sundial.datetime))
```

Definition at line 941 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- rpki_engine.py (3107)

14.184 rpki.rpki_engine.publication_queue Class Reference

Inherits object.

Collaboration diagram for rpki.rpki_engine.publication_queue:

Public Member Functions

- def __init__
- def call_pubd
- def publish
- def withdraw

Public Attributes

- handlers
- msgs
- repositories
- uris

Static Public Attributes

- replace = True

Private Member Functions

- def _add

14.184.1 Detailed Description

```
Utility to simplify publication from within rpkid.

General idea here is to accumulate a collection of objects to be
published, in one or more repositories, each potentially with its
own completion callback.  Eventually we want to publish everything
we've accumulated, at which point we need to iterate over the
collection and do repository.call_pubd() for each repository.
```

Definition at line 1366 of file rpki_engine.py.

14.184.2 Member Function Documentation

14.184.2.1 def rpki.rpki_engine.publication_queue.__init__ (*self*)

Definition at line 1379 of file rpki_engine.py.

14.184.2.2 def rpki.rpki_engine.publication_queue._add (*self*, *cls*, *uri*, *obj*, *repository*, *handler*, *withdraw*) [private]

Definition at line 1386 of file rpki_engine.py.

14.184.2.3 def rpki.rpki_engine.publication_queue.call_pubd (*self*, *cb*, *eb*)

Definition at line 1409 of file rpki_engine.py.

14.184.2.4 def rpki.rpki_engine.publication_queue.publish (*self*, *cls*, *uri*, *obj*, *repository*, *handler* = None)

Definition at line 1403 of file rpki_engine.py.

14.184.2.5 def rpki.rpki_engine.publication_queue.withdraw (*self*, *cls*, *uri*, *obj*, *repository*, *handler* = `None`)

Definition at line 1406 of file rpki_engine.py.

14.184.3 Member Data Documentation

14.184.3.1 rpki.rpki_engine.publication_queue.handlers

Definition at line 1382 of file rpki_engine.py.

14.184.3.2 rpki.rpki_engine.publication_queue.msgs

Definition at line 1381 of file rpki_engine.py.

14.184.3.3 rpki.rpki_engine.publication_queue.replace = True `[static]`

Definition at line 1377 of file rpki_engine.py.

14.184.3.4 rpki.rpki_engine.publication_queue.repositories

Definition at line 1380 of file rpki_engine.py.

14.184.3.5 rpki.rpki_engine.publication_queue.uris

Definition at line 1384 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- rpki_engine.py (3107)

14.185 rpki.rpki_engine.revoked_cert_obj Class Reference

Inherits rpki::sql::sql_persistent.

Collaboration diagram for rpki.rpki_engine.revoked_cert_obj:

Public Member Functions

- def __init__
- def ca_detail

- def revoke

Public Attributes

- ca_detail_id
- expires
- gctx
- revoked
- serial

Static Public Attributes

- tuple sql_template

14.185.1 Detailed Description

```
Tombstone for a revoked certificate.
```

Definition at line 1088 of file rpki_engine.py.

14.185.2 Member Function Documentation

14.185.2.1 def rpki.rpki_engine.revoked_cert_obj.__init__ (*self*, *gctx* = `None`, *serial* = `None`, *revoked* = `None`, *expires* = `None`, *ca_detail_id* = `None`)

```
Initialize a revoked_cert_obj.
```

Definition at line 1101 of file rpki_engine.py.

14.185.2.2 def rpki.rpki_engine.revoked_cert_obj.ca_detail (*self*)

```
Fetch ca_detail object to which this revoked_cert_obj links.
```

Definition at line 1112 of file rpki_engine.py.

14.185.2.3 def rpki.rpki_engine.revoked_cert_obj.revoke (*cls*, *cert*, *ca_detail*)

```
Revoke a certificate.
```

Definition at line 1117 of file rpki_engine.py.

14.185.3 Member Data Documentation

14.185.3.1 rpki.rpki_engine.revoked_cert_obj.ca_detail_id

Definition at line 1108 of file rpki_engine.py.

14.185.3.2 rpki.rpki_engine.revoked_cert_obj.expires

Definition at line 1107 of file rpki_engine.py.

14.185.3.3 rpki.rpki_engine.revoked_cert_obj.gctx

Reimplemented from rpki.sql.sql_persistent.

Definition at line 1104 of file rpki_engine.py.

14.185.3.4 rpki.rpki_engine.revoked_cert_obj.revoked

Definition at line 1106 of file rpki_engine.py.

14.185.3.5 rpki.rpki_engine.revoked_cert_obj.serial

Definition at line 1105 of file rpki_engine.py.

14.185.3.6 tuple rpki.rpki_engine.revoked_cert_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
    "revoked_cert",
    "revoked_cert_id",
    "serial",
    "ca_detail_id",
    ("revoked", rpki.sundial.datetime),
    ("expires", rpki.sundial.datetime))
```

Definition at line 1093 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- rpki_engine.py (3107)

14.186 rpki.rpki_engine.roa_obj Class Reference

Inherits rpki::sql::sql_persistent.

Collaboration diagram for rpki.rpki_engine.roa_obj:

Public Member Functions

- def __init__
- def ca_detail
- def generate
- def published_callback
- def regenerate

- def revoke
- def self
- def sql_delete_hook
- def sql_fetch_hook
- def sql_insert_hook
- def update
- def uri
- def uri_tail

Public Attributes

- asn
- gctx
- ipv4
- ipv6
- self_id

Static Public Attributes

- ca_detail_id = None
- cert = None
- published = None
- roa = None
- tuple sql_template

14.186.1 Detailed Description

```
Route Origin Authorization.
```

Definition at line 1128 of file rpki_engine.py.

14.186.2 Member Function Documentation

14.186.2.1 def rpki.rpki_engine.roa_obj.__init__ (*self*, *gctx* = `None`, *self_id* = `None`, *asn* = `None`, *ipv4* = `None`, *ipv6* = `None`)

Definition at line 1194 of file rpki_engine.py.

14.186.2.2 def rpki.rpki_engine.roa_obj.ca_detail (*self*)

```
Fetch ca_detail object to which this roa_obj links.
```

Definition at line 1154 of file rpki_engine.py.

14.186.2.3 def rpki.rpki_engine.roa_obj.generate (*self*, *publisher*)

```
Generate a ROA.

At present this does not support ROAs with multiple signatures
(neither does the current CMS code).

At present we have no way of performing a direct lookup from a
desired set of resources to a covering certificate, so we have to
search.  This could be quite slow if we have a lot of active
ca_detail objects.  Punt on the issue for now, revisit if
profiling shows this as a hotspot.

Once we have the right covering certificate, we generate the ROA
payload, generate a new EE certificate, use the EE certificate to
sign the ROA payload, publish the result, then throw away the
private key for the EE cert, all per the ROA specification.  This
implies that generating a lot of ROAs will tend to thrash
/dev/random, but there is not much we can do about that.
```

Definition at line 1237 of file rpki_engine.py.

14.186.2.4 def rpki.rpki_engine.roa_obj.published_callback (*self*, *pdu*)

```
Check publication result.
```

Definition at line 1303 of file rpki_engine.py.

14.186.2.5 def rpki.rpki_engine.roa_obj.regenerate (*self*, *publisher*)

```
Reissue ROA associated with this roa_obj.
```

Definition at line 1343 of file rpki_engine.py.

14.186.2.6 def rpki.rpki_engine.roa_obj.revoke (*self*, *publisher*, *regenerate* = `False`, *allow_failure* = `False`)

```
Withdraw ROA associated with this roa_obj.

In order to preserve make-before-break properties without
duplicating code, this method also handles generating a
replacement ROA when requested.

If allow_failure is set, failing to withdraw the ROA will not be
considered an error.
```

Definition at line 1311 of file rpki_engine.py.

14.186.2.7 def rpki.rpki_engine.roa_obj.self (*self*)

```
Fetch self object to which this roa_obj links.
```

Definition at line 1148 of file rpki_engine.py.

14.186.2.8 def rpki.rpki_engine.roa_obj.sql_delete_hook (*self*)

```
Extra SQL delete actions for roa_obj -- handle prefix lists.
```

Reimplemented from rpki.sql.sql_persistent.

Definition at line 1188 of file rpki_engine.py.

14.186.2.9 def rpki.rpki_engine.roa_obj.sql_fetch_hook (*self*)

```
Extra SQL fetch actions for roa_obj -- handle prefix lists.
```

Reimplemented from rpki.sql.sql_persistent.

Definition at line 1160 of file rpki_engine.py.

14.186.2.10 def rpki.rpki_engine.roa_obj.sql_insert_hook (*self*)

```
Extra SQL insert actions for roa_obj -- handle prefix lists.
```

Reimplemented from rpki.sql.sql_persistent.

Definition at line 1174 of file rpki_engine.py.

14.186.2.11 def rpki.rpki_engine.roa_obj.update (*self*, *publisher*)

```
Bring this roa_obj's ROA up to date if necesssary.
```

Definition at line 1207 of file rpki_engine.py.

14.186.2.12 def rpki.rpki_engine.roa_obj.uri (*self*, *key* = `None`)

```
Return the publication URI for this roa_obj's ROA.
```

Definition at line 1352 of file rpki_engine.py.

14.186.2.13 def rpki.rpki_engine.roa_obj.uri_tail (*self*, *key* = `None`)

```
Return the tail (filename portion) of the publication URI for this
roa_obj's ROA.
```

Definition at line 1358 of file rpki_engine.py.

14.186.3 Member Data Documentation

14.186.3.1 rpki.rpki_engine.roa_obj.asn

Definition at line 1198 of file rpki_engine.py.

14.186.3.2 rpki.rpki_engine.roa_obj.ca_detail_id = None `[static]`

Definition at line 1143 of file rpki_engine.py.

14.186.3.3 rpki.rpki_engine.roa_obj.cert = None [static]

Definition at line 1144 of file rpki_engine.py.

14.186.3.4 rpki.rpki_engine.roa_obj.gctx

Reimplemented from rpki.sql.sql_persistent.

Definition at line 1196 of file rpki_engine.py.

14.186.3.5 rpki.rpki_engine.roa_obj.ipv4

Definition at line 1199 of file rpki_engine.py.

14.186.3.6 rpki.rpki_engine.roa_obj.ipv6

Definition at line 1200 of file rpki_engine.py.

14.186.3.7 rpki.rpki_engine.roa_obj.published = None [static]

Definition at line 1146 of file rpki_engine.py.

14.186.3.8 rpki.rpki_engine.roa_obj.roa = None [static]

Definition at line 1145 of file rpki_engine.py.

14.186.3.9 rpki.rpki_engine.roa_obj.self_id

Definition at line 1197 of file rpki_engine.py.

14.186.3.10 tuple rpki.rpki_engine.roa_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
    "roa",
    "roa_id",
    "ca_detail_id",
    "self_id",
    "asn",
    ("roa", rpki.x509.ROA),
    ("cert", rpki.x509.X509),
    ("published", rpki.sundial.datetime))
```

Definition at line 1133 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- rpki_engine.py (3107)

14.187 rpki.rpki_engine.rpkid_context Class Reference

Inherits object.

Collaboration diagram for rpki.rpki_engine.rpkid_context:

Public Member Functions

- def __init__
- def build_https_ta_cache
- def checkpoint
- def clear_https_ta_cache
- def cron

- def cronjob_handler
- def irdb_query
- def irdb_query_child_resources
- def irdb_query_roa_requests
- def left_right_handler
- def start_cron
- def up_down_handler

Public Attributes

- bpki_ta
- cron_keepalive
- cron_period
- cron_timeout
- cron_timer
- https_server_host
- https_server_port
- initial_delay
- irbe_cert
- irdb_cert
- irdb_url
- publication_kludge_base
- rpkid_cert
- rpkid_key
- sql
- use_internal_cron

Static Public Attributes

- https_ta_cache = None

  HTTPS trust anchor cache, to avoid regenerating it for every TLS connection.

- tuple up_down_url_regexp = re.compile("/up-down/([-A-Z0-9_]+)/([-A-Z0-9_-]+)$", re.I)

14.187.1 Detailed Description

```
A container for various global rpkid parameters.
```

Definition at line 39 of file rpki_engine.py.

14.187.2 Member Function Documentation

14.187.2.1 def rpki.rpki_engine.rpkid_context.__init__ (*self*, *cfg*)

Definition at line 44 of file rpki_engine.py.

14.187.2.2 def rpki.rpki_engine.rpkid_context.build_https_ta_cache (*self*)

```
Build dynamic TLS trust anchors.
```

Definition at line 288 of file rpki_engine.py.

14.187.2.3 def rpki.rpki_engine.rpkid_context.checkpoint (*self*)

```
Record that we were still alive when we got here, by resetting
keepalive timer.
```

Definition at line 200 of file rpki_engine.py.

14.187.2.4 def rpki.rpki_engine.rpkid_context.clear_https_ta_cache (*self*)

```
Clear dynamic TLS trust anchors.
```

Definition at line 279 of file rpki_engine.py.

14.187.2.5 def rpki.rpki_engine.rpkid_context.cron (*self*, *cb* = `None`)

```
Periodic tasks.
```

Definition at line 207 of file rpki_engine.py.

14.187.2.6 def rpki.rpki_engine.rpkid_context.cronjob_handler (*self*, *query*, *path*, *cb*)

```
External trigger for periodic tasks.  This is somewhat obsolete
now that we have internal timers, but the test framework still
uses it.
```

Definition at line 263 of file rpki_engine.py.

14.187.2.7 def rpki.rpki_engine.rpkid_context.irdb_query (*self*, *q_pdu*, *callback*, *errback*)

```
Perform an IRDB callback query.
```

Definition at line 86 of file rpki_engine.py.

14.187.2.8 def rpki.rpki_engine.rpkid_context.irdb_query_child_resources (*self*, *self_handle*, *child_handle*, *callback*, *errback*)

```
Ask IRDB about a child's resources.
```

Definition at line 112 of file rpki_engine.py.

14.187.2.9 def rpki.rpki_engine.rpkid_context.irdb_query_roa_requests (*self*, *self_handle*, *callback*, *errback*)

```
Ask IRDB about self's ROA requests.
```

Definition at line 134 of file rpki_engine.py.

14.187.2.10 def rpki.rpki_engine.rpkid_context.left_right_handler (*self*, *query*, *path*, *cb*)

```
Process one left-right PDU.
```

Definition at line 146 of file rpki_engine.py.

14.187.2.11 def rpki.rpki_engine.rpkid_context.start_cron (*self*)

```
Start clock for rpkid's internal cron process.
```

Definition at line 73 of file rpki_engine.py.

14.187.2.12 def rpki.rpki_engine.rpkid_context.up_down_handler (*self*, *query*, *path*, *cb*)

```
Process one up-down PDU.
```

Definition at line 172 of file rpki_engine.py.

14.187.3 Member Data Documentation

14.187.3.1 rpki.rpki_engine.rpkid_context.bpki_ta

Definition at line 48 of file rpki_engine.py.

14.187.3.2 rpki.rpki_engine.rpkid_context.cron_keepalive

Definition at line 68 of file rpki_engine.py.

14.187.3.3 rpki.rpki_engine.rpkid_context.cron_period

Definition at line 67 of file rpki_engine.py.

14.187.3.4 rpki.rpki_engine.rpkid_context.cron_timeout

Definition at line 71 of file rpki_engine.py.

14.187.3.5 rpki.rpki_engine.rpkid_context.cron_timer

Definition at line 79 of file rpki_engine.py.

14.187.3.6 rpki.rpki_engine.rpkid_context.https_server_host

Definition at line 56 of file rpki_engine.py.

14.187.3.7 rpki.rpki_engine.rpkid_context.https_server_port

Definition at line 57 of file rpki_engine.py.

14.187.3.8 rpki::rpki_engine.rpkid_context::https_ta_cache = None [static]

HTTPS trust anchor cache, to avoid regenerating it for every TLS connection.

Definition at line 277 of file rpki_engine.py.

14.187.3.9 rpki.rpki_engine.rpkid_context.initial_delay

Definition at line 63 of file rpki_engine.py.

14.187.3.10 rpki.rpki_engine.rpkid_context.irbe_cert

Definition at line 50 of file rpki_engine.py.

14.187.3.11 rpki.rpki_engine.rpkid_context.irdb_cert

Definition at line 49 of file rpki_engine.py.

14.187.3.12 rpki.rpki_engine.rpkid_context.irdb_url

Definition at line 54 of file rpki_engine.py.

14.187.3.13 rpki.rpki_engine.rpkid_context.publication_kludge_base

Definition at line 59 of file rpki_engine.py.

14.187.3.14 rpki.rpki_engine.rpkid_context.rpkid_cert

Definition at line 51 of file rpki_engine.py.

14.187.3.15 rpki.rpki_engine.rpkid_context.rpkid_key

Definition at line 52 of file rpki_engine.py.

14.187.3.16 rpki.rpki_engine.rpkid_context.sql

Definition at line 46 of file rpki_engine.py.

14.187.3.17 tuple rpki.rpki_engine.rpkid_context.up_down_url_regexp = re.compile("/up-down/([-A-Z0-9_]+)/([-A-Z0-9_]+)$", re.I) `[static]`

Definition at line 170 of file rpki_engine.py.

14.187.3.18 rpki.rpki_engine.rpkid_context.use_internal_cron

Definition at line 61 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- rpki_engine.py (3107)

14.188 rpki.sql.session Class Reference

Inherits object.

Collaboration diagram for rpki.sql.session:

Public Member Functions

- def __init__
- def assert_pristine
- def cache_clear
- def close
- def connect
- def execute
- def executemany
- def fetchall
- def lastrowid
- def ping
- def sweep

Public Attributes

- cache
- cur
- database
- db
- dirty
- password
- username

Private Member Functions

- def _wrap_execute

Static Private Attributes

- _exceptions_enabled = False

14.188.1 Detailed Description

```
SQL session layer.
```

Definition at line 50 of file sql.py.

14.188.2 Member Function Documentation

14.188.2.1 def rpki.sql.session.__init__ (*self*, *cfg*)

Definition at line 57 of file sql.py.

14.188.2.2 def rpki.sql.session._wrap_execute (*self*, *func*, *query*, *args*) [private]

Definition at line 88 of file sql.py.

14.188.2.3 def rpki.sql.session.assert_pristine (*self*)

```
Assert that there are no dirty objects in the cache.
```

Definition at line 112 of file sql.py.

14.188.2.4 def rpki.sql.session.cache_clear (*self*)

```
Clear the object cache.
```

Definition at line 108 of file sql.py.

14.188.2.5 def rpki.sql.session.close (*self*)

Definition at line 77 of file sql.py.

14.188.2.6 def rpki.sql.session.connect (*self*)

Definition at line 72 of file sql.py.

14.188.2.7 def rpki.sql.session.execute (*self*, *query*, *args* = `None`)

Definition at line 96 of file sql.py.

14.188.2.8 def rpki.sql.session.executemany (*self*, *query*, *args*)

Definition at line 99 of file sql.py.

14.188.2.9 def rpki.sql.session.fetchall (*self*)

Definition at line 102 of file sql.py.

14.188.2.10 def rpki.sql.session.lastrowid (*self*)

Definition at line 105 of file sql.py.

14.188.2.11 def rpki.sql.session.ping (*self*)

Definition at line 85 of file sql.py.

14.188.2.12 def rpki.sql.session.sweep (*self*)

```
Write any dirty objects out to SQL.
```

Definition at line 116 of file sql.py.

14.188.3 Member Data Documentation

14.188.3.1 rpki.sql.session._exceptions_enabled = False [static, private]

Definition at line 55 of file sql.py.

14.188.3.2 rpki.sql.session.cache

Definition at line 67 of file sql.py.

14.188.3.3 rpki.sql.session.cur

Definition at line 74 of file sql.py.

14.188.3.4 rpki.sql.session.database

Definition at line 64 of file sql.py.

14.188.3.5 rpki.sql.session.db

Definition at line 73 of file sql.py.

14.188.3.6 rpki.sql.session.dirty

Definition at line 68 of file sql.py.

14.188.3.7 rpki.sql.session.password

Definition at line 65 of file sql.py.

14.188.3.8 rpki.sql.session.username

Definition at line 63 of file sql.py.

The documentation for this class was generated from the following file:

- sql.py (2895)

14.189 rpki.sql.sql_persistent Class Reference

Inherits object.

Inherited by rpki.left_right.data_elt, rpki.publication.control_elt, rpki.rpki_engine.ca_-detail_obj, rpki.rpki_engine.ca_obj, rpki.rpki_engine.child_cert_obj, rpki.rpki_-engine.revoked_cert_obj, and rpki.rpki_engine.roa_obj.

Collaboration diagram for rpki.sql.sql_persistent:

Public Member Functions

- def sql_decode
- def sql_delete
- def sql_delete_hook
- def sql_encode
- def sql_fetch

- def sql_fetch_all
- def sql_fetch_hook
- def sql_fetch_where
- def sql_fetch_where1
- def sql_init
- def sql_insert_hook
- def sql_is_dirty
- def sql_mark_clean
- def sql_mark_deleted
- def sql_mark_dirty
- def sql_store
- def sql_update_hook

Public Attributes

- gctx

Static Public Attributes

- sql_debug = False

  Enable logging of SQL actions.

- sql_deleted = False

  Whether our cached copy of this object has been deleted.

- sql_in_db = False

  Whether this object is already in SQL or not.

14.189.1 Detailed Description

```
Mixin for persistent class that needs to be stored in SQL.
```

Definition at line 152 of file sql.py.

14.189.2 Member Function Documentation

14.189.2.1 def rpki.sql.sql_persistent.sql_decode (*self*, *vals*)

```
Initialize an object with values returned by self.sql_fetch().
This is a default version that assumes a one-to-one mapping
between column names in SQL and attribute names in Python.  If you
need something fancier, override this.
```

Reimplemented in rpki.rpki_engine.ca_detail_obj.

Definition at line 322 of file sql.py.

14.189.2.2 def rpki.sql.sql_persistent.sql_delete (*self*)

```
Delete this object from SQL.
```

Definition at line 293 of file sql.py.

14.189.2.3 def rpki.sql.sql_persistent.sql_delete_hook (*self*)

```
Customization hook.
```

Reimplemented in rpki.rpki_engine.roa_obj.

Definition at line 348 of file sql.py.

14.189.2.4 def rpki.sql.sql_persistent.sql_encode (*self*)

```
Convert object attributes into a dict for use with canned SQL
queries.  This is a default version that assumes a one-to-one
mapping between column names in SQL and attribute names in Python.
If you need something fancier, override this.
```

Definition at line 309 of file sql.py.

14.189.2.5 def rpki.sql.sql_persistent.sql_fetch (*cls*, *gctx*, *id*)

```
Fetch one object from SQL, based on its primary key.

Since in this one case we know that the primary index is also the
cache key, we check for a cache hit directly in the hope of
bypassing the SQL lookup entirely.
```

```
This method is usually called via a one-line class-specific
wrapper.  As a convenience, we also accept an id of None, and just
return None in this case.
```

Definition at line 173 of file sql.py.

14.189.2.6 def rpki.sql.sql_persistent.sql_fetch_all (*cls*, *gctx*)

```
Fetch all objects of this type from SQL.
```

Definition at line 211 of file sql.py.

14.189.2.7 def rpki.sql.sql_persistent.sql_fetch_hook (*self*)

```
Customization hook.
```

Reimplemented in rpki.rpki_engine.roa_obj.

Definition at line 335 of file sql.py.

14.189.2.8 def rpki.sql.sql_persistent.sql_fetch_where (*cls*, *gctx*, *where*, *args* = `None`, *also_from* = `None`)

```
Fetch objects of this type matching an arbitrary SQL WHERE expression.
```

Definition at line 216 of file sql.py.

14.189.2.9 def rpki.sql.sql_persistent.sql_fetch_where1 (*cls*, *gctx*, *where*, *args* = `None`, *also_from* = `None`)

```
Fetch one object from SQL, based on an arbitrary SQL WHERE expression.
```

Definition at line 196 of file sql.py.

14.189.2.10 def rpki.sql.sql_persistent.sql_init (*cls*, *gctx*, *row*, *key*)

```
Initialize one Python object from the result of a SQL query.
```

Definition at line 243 of file sql.py.

14.189.2.11 def rpki.sql.sql_persistent.sql_insert_hook (*self*)

```
Customization hook.
```

Reimplemented in rpki.rpki_engine.roa_obj.

Definition at line 339 of file sql.py.

14.189.2.12 def rpki.sql.sql_persistent.sql_is_dirty (*self*)

```
Query whether this object needs to be written back to SQL.
```

Definition at line 263 of file sql.py.

14.189.2.13 def rpki.sql.sql_persistent.sql_mark_clean (*self*)

```
Mark this object as not needing to be written back to SQL.
```

Definition at line 259 of file sql.py.

14.189.2.14 def rpki.sql.sql_persistent.sql_mark_deleted (*self*)

```
Mark this object as needing to be deleted in SQL.
```

Definition at line 267 of file sql.py.

14.189.2.15 def rpki.sql.sql_persistent.sql_mark_dirty (*self*)

```
Mark this object as needing to be written back to SQL.
```

Definition at line 255 of file sql.py.

14.189.2.16 def rpki.sql.sql_persistent.sql_store (*self*)

```
Store this object to SQL.
```

Definition at line 271 of file sql.py.

14.189.2.17 def rpki.sql.sql_persistent.sql_update_hook (*self*)

```
Customization hook.
```

Definition at line 343 of file sql.py.

14.189.3 Member Data Documentation

14.189.3.1 rpki.sql.sql_persistent.gctx

Reimplemented in rpki.rpki_engine.ca_obj, rpki.rpki_engine.ca_detail_obj, rpki.rpki_engine.child_cert_obj, rpki.rpki_engine.revoked_cert_obj, and rpki.rpki_-engine.roa_obj.

Definition at line 248 of file sql.py.

14.189.3.2 rpki::sql.sql_persistent::sql_debug = False [static]

Enable logging of SQL actions.

Definition at line 170 of file sql.py.

14.189.3.3 rpki::sql.sql_persistent::sql_deleted = False [static]

Whether our cached copy of this object has been deleted.

Definition at line 165 of file sql.py.

14.189.3.4 rpki::sql.sql_persistent::sql_in_db = False [static]

Whether this object is already in SQL or not.

Definition at line 160 of file sql.py.

The documentation for this class was generated from the following file:

- sql.py (2895)

14.190 rpki.sql.template Class Reference

Inherits object.

Collaboration diagram for rpki.sql.template:

Public Member Functions

- def __init__

Public Attributes

- columns
- delete
- index
- insert
- map

- select
- table
- update

14.190.1 Detailed Description

```
SQL template generator.
```

Definition at line 128 of file sql.py.

14.190.2 Member Function Documentation

14.190.2.1 def rpki.sql.template.__init__ (*self*, *table_name*, *index_column*, *data_columns*)

```
Build a SQL template.
```

Definition at line 133 of file sql.py.

14.190.3 Member Data Documentation

14.190.3.1 rpki.sql.template.columns

Definition at line 140 of file sql.py.

14.190.3.2 rpki.sql.template.delete

Definition at line 150 of file sql.py.

14.190.3.3 rpki.sql.template.index

Definition at line 139 of file sql.py.

14.190.3.4 rpki.sql.template.insert

Definition at line 143 of file sql.py.

14.190.3.5 rpki.sql.template.map

Definition at line 141 of file sql.py.

14.190.3.6 rpki.sql.template.select

Definition at line 142 of file sql.py.

14.190.3.7 rpki.sql.template.table

Definition at line 138 of file sql.py.

14.190.3.8 rpki.sql.template.update

Definition at line 146 of file sql.py.

The documentation for this class was generated from the following file:

- sql.py (2895)

14.191 rpki.sundial.datetime Class Reference

Inherits pydatetime::datetime.

Collaboration diagram for rpki.sundial.datetime:

Public Member Functions

- def __add__
- def __radd__
- def __rsub__
- def __str__
- def __sub__

- def earlier
- def from_sql
- def fromASN1tuple
- def fromdatetime
- def fromGeneralizedTime
- def fromUTCTime
- def fromXMLtime
- def later
- def to_sql
- def toASN1tuple
- def toGeneralizedTime
- def totimestamp
- def toUTCTime
- def toXMLtime

Static Public Attributes

- tuple PKIX_threshhold = pydatetime.datetime(2050, 1, 1)

  Threshold specified in RFC 3280 for switchover from UTCTime to GeneralizedTime.

14.191.1 Detailed Description

```
RPKI extensions to standard datetime.datetime class.  All work here
is in UTC, so we use naive datetime objects.
```

Definition at line 54 of file sundial.py.

14.191.2 Member Function Documentation

14.191.2.1 def rpki.sundial.datetime.__add__ (*self*, *y*)

Definition at line 163 of file sundial.py.

14.191.2.2 def rpki.sundial.datetime.__radd__ (*self*, *y*)

Definition at line 164 of file sundial.py.

14.191.2.3 def rpki.sundial.datetime.__rsub__ (*self*, *y*)

Definition at line 165 of file sundial.py.

14.191.2.4 def rpki.sundial.datetime.__str__ (*self*)

Definition at line 124 of file sundial.py.

14.191.2.5 def rpki.sundial.datetime.__sub__ (*self*, *y*)

Definition at line 166 of file sundial.py.

14.191.2.6 def rpki.sundial.datetime.earlier (*self*, *other*)

```
Return the earlier of two timestamps.
```

Definition at line 159 of file sundial.py.

14.191.2.7 def rpki.sundial.datetime.from_sql (*cls*, *x*)

```
Convert from SQL storage format.
```

Definition at line 136 of file sundial.py.

14.191.2.8 def rpki.sundial.datetime.fromASN1tuple (*cls*, *x*)

```
Convert from ASN.1 tuple representation.
```

Definition at line 86 of file sundial.py.

14.191.2.9 def rpki.sundial.datetime.fromdatetime (*cls*, *x*)

```
Convert a datetime.datetime object into this subclass.  This is
whacky due to the weird constructors for datetime.
```

Definition at line 128 of file sundial.py.

14.191.2.10 def rpki.sundial.datetime.fromGeneralizedTime (*cls*, *x*)

```
Convert from ASN.1 GeneralizedTime.
```

Definition at line 77 of file sundial.py.

14.191.2.11 def rpki.sundial.datetime.fromUTCTime (*cls*, *x*)

```
Convert from ASN.1 UTCTime.
```

Definition at line 68 of file sundial.py.

14.191.2.12 def rpki.sundial.datetime.fromXMLtime (*cls*, *x*)

```
Convert from XML time representation.
```

Definition at line 111 of file sundial.py.

14.191.2.13 def rpki.sundial.datetime.later (*self*, *other*)

```
Return the later of two timestamps.
```

Definition at line 155 of file sundial.py.

14.191.2.14 def rpki.sundial.datetime.to_sql (*self*)

```
Convert to SQL storage format.

There's something whacky going on in the MySQLdb module, it throws
range errors when storing a derived type into a DATETIME column.
Investigate some day, but for now brute force this by copying the
relevant fields into a datetime.datetime for MySQLdb's
consumption.
```

Definition at line 140 of file sundial.py.

14.191.2.15 def rpki.sundial.datetime.toASN1tuple (*self*)

```
Convert to ASN.1 tuple representation.
```

Definition at line 101 of file sundial.py.

14.191.2.16 def rpki.sundial.datetime.toGeneralizedTime (*self*)

```
Convert to ASN.1 GeneralizedTime.
```

Definition at line 81 of file sundial.py.

14.191.2.17 def rpki.sundial.datetime.totimestamp (*self*)

```
Convert to seconds from epoch (like time.time()).  Conversion
method is a bit silly, but avoids time module timezone whackiness.
```

Definition at line 60 of file sundial.py.

14.191.2.18 def rpki.sundial.datetime.toUTCTime (*self*)

```
Convert to ASN.1 UTCTime.
```

Definition at line 72 of file sundial.py.

14.191.2.19 def rpki.sundial.datetime.toXMLtime (*self*)

```
Convert to XML time representation.
```

Definition at line 120 of file sundial.py.

14.191.3 Member Data Documentation

14.191.3.1 rpki::sundial.datetime::PKIX_threshhold = pydatetime.datetime(2050, 1, 1) [static]

Threshold specified in RFC 3280 for switchover from UTCTime to GeneralizedTime.

Definition at line 99 of file sundial.py.

The documentation for this class was generated from the following file:

- sundial.py (3191)

14.192 rpki.sundial.timedelta Class Reference

Inherits pydatetime::timedelta.

Collaboration diagram for rpki.sundial.timedelta:

Public Member Functions

- def __abs__
- def __add__
- def __div__
- def __floordiv__
- def __mul__

- def __neg__
- def __pos__
- def __radd__
- def __rdiv__
- def __rfloordiv__
- def __rmul__
- def __rsub__
- def __sub__
- def convert_to_seconds
- def fromtimedelta
- def parse

Static Public Attributes

- tuple regexp

  Hideously ugly regular expression to parse the complex text form.

- int years_to_seconds = 31556926

  Conversion factor from years to seconds (value furnished by the "units" program).

14.192.1 Detailed Description

```
Timedelta with text parsing.  This accepts two input formats:

- A simple integer, indicating a number of seconds.

- A string of the form "uY vW wD xH yM zS" where u, v, w, x, y, and z
  are integers and Y, W, D, H, M, and S indicate years, weeks, days,
  hours, minutes, and seconds.  All of the fields are optional, but
  at least one must be specified.  Eg,"3D4H" means "three days plus
  four hours".

There is no "months" format, because the definition of a month is too
fuzzy to be useful (what day is six months from August 30th?)

Similarly, the "years" conversion may produce surprising results, as
"one year" in conventional English does not refer to a fixed interval
but rather a fixed (and in some cases undefined) offset within the
Gregorian calendar (what day is one year from February 29th?)  1Y as
implemented by this code refers to a specific number of seconds.
If you mean 365 days or 52 weeks, say that instead.
```

Definition at line 168 of file sundial.py.

14.192.2 Member Function Documentation

14.192.2.1 def rpki.sundial.timedelta.__abs__ (*self*)

Definition at line 243 of file sundial.py.

14.192.2.2 def rpki.sundial.timedelta.__add__ (*self*, *x*)

Definition at line 244 of file sundial.py.

14.192.2.3 def rpki.sundial.timedelta.__div__ (*self*, *x*)

Definition at line 245 of file sundial.py.

14.192.2.4 def rpki.sundial.timedelta.__floordiv__ (*self*, *x*)

Definition at line 246 of file sundial.py.

14.192.2.5 def rpki.sundial.timedelta.__mul__ (*self*, *x*)

Definition at line 247 of file sundial.py.

14.192.2.6 def rpki.sundial.timedelta.__neg__ (*self*)

Definition at line 248 of file sundial.py.

14.192.2.7 def rpki.sundial.timedelta.__pos__ (*self*)

Definition at line 249 of file sundial.py.

14.192.2.8 def rpki.sundial.timedelta.__radd__ (*self*, *x*)

Definition at line 250 of file sundial.py.

14.192.2.9 def rpki.sundial.timedelta.__rdiv__ (*self*, *x*)

Definition at line 251 of file sundial.py.

14.192.2.10 def rpki.sundial.timedelta.__rfloordiv__ (*self*, *x*)

Definition at line 252 of file sundial.py.

14.192.2.11 def rpki.sundial.timedelta.__rmul__ (*self*, *x*)

Definition at line 253 of file sundial.py.

14.192.2.12 def rpki.sundial.timedelta.__rsub__ (*self*, *x*)

Definition at line 254 of file sundial.py.

14.192.2.13 def rpki.sundial.timedelta.__sub__ (*self*, *x*)

Definition at line 255 of file sundial.py.

14.192.2.14 def rpki.sundial.timedelta.convert_to_seconds (*self*)

```
Convert a timedelta interval to seconds.
```

Definition at line 234 of file sundial.py.

14.192.2.15 def rpki.sundial.timedelta.fromtimedelta (*cls*, *x*)

```
Convert a datetime.timedelta object into this subclass.
```

Definition at line 239 of file sundial.py.

14.192.2.16 def rpki.sundial.timedelta.parse (*cls*, *arg*)

```
Parse text into a timedelta object.
```

Definition at line 213 of file sundial.py.

14.192.3 Member Data Documentation

14.192.3.1 rpki::sundial.timedelta::regexp [static]

Initial value:

```
re.compile("\\s*".join(("^",
                                    "(?:(?P<years>\\d+)Y)?",
                                    "(?:(?P<weeks>\\d+)W)?",
                                    "(?:(?P<days>\\d+)D)?",
                                    "(?:(?P<hours>\\d+)H)?",
                                    "(?:(?P<minutes>\\d+)M)?",
                                    "(?:(?P<seconds>\\d+)S)?",
                                    "$")),
                       re.I)
```

Hideously ugly regular expression to parse the complex text form.

Tags are intended for use with re.MatchObject.groupdict() and map directly to the keywords expected by the timedelta constructor.

Definition at line 196 of file sundial.py.

14.192.3.2 rpki::sundial.timedelta::years_to_seconds = 31556926 [static]

Conversion factor from years to seconds (value furnished by the "units" program).

Definition at line 210 of file sundial.py.

The documentation for this class was generated from the following file:

- sundial.py (3191)

14.193 rpki.up_down.base_elt Class Reference

Inherits object.

Inherited by rpki.up_down.certificate_elt, rpki.up_down.class_elt, rpki.up_down.class_response_syntax, rpki.up_down.error_response_pdu, rpki.up_down.issue_pdu, rpki.up_down.list_pdu, rpki.up_down.message_pdu, and rpki.up_down.revoke_syntax.

Collaboration diagram for rpki.up_down.base_elt:

Public Member Functions

- def check_response
- def endElement
- def make_b64elt
- def make_elt
- def serve_pdu
- def startElement

14.193.1 Detailed Description

```
Generic PDU object.

Virtual class, just provides some default methods.
```

Definition at line 43 of file up_down.py.

14.193.2 Member Function Documentation

14.193.2.1 def rpki.up_down.base_elt.check_response (*self*)

```
Placeholder for response checking.
```

Reimplemented in rpki.up_down.issue_response_pdu, and rpki.up_down.error_response_pdu.

Definition at line 91 of file up_down.py.

14.193.2.2 def rpki.up_down.base_elt.endElement (*self*, *stack*, *name*, *text*)

```
Ignore endElement() if there's no specific handler.

If we don't need to do anything else, just pop the stack.
```

Reimplemented in rpki.up_down.certificate_elt, rpki.up_down.class_elt, rpki.up_down.issue_pdu, and rpki.up_down.error_response_pdu.

Definition at line 59 of file up_down.py.

14.193.2.3 def rpki.up_down.base_elt.make_b64elt (*self*, *elt*, *name*, *value* = `None`)

```
Construct a sub-element with Base64 text content.
```

Definition at line 78 of file up_down.py.

14.193.2.4 def rpki.up_down.base_elt.make_elt (*self*, *name*, *attrs*)

```
Construct a element, copying over a set of attributes.
```

Definition at line 67 of file up_down.py.

14.193.2.5 def rpki.up_down.base_elt.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *callback*, *errback*)

```
Default PDU handler to catch unexpected types.
```

Reimplemented in rpki.up_down.list_pdu, rpki.up_down.issue_pdu, rpki.up_down.revoke_pdu, rootd.list_pdu, rootd.issue_pdu, and rootd.revoke_pdu.

Definition at line 87 of file up_down.py.

14.193.2.6 def rpki.up_down.base_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Ignore startElement() if there's no specific handler.

Some elements have no attributes and we only care about their
text content.
```

Reimplemented in rpki.up_down.certificate_elt, rpki.up_down.class_elt, rpki.up_down.class_response_syntax, rpki.up_down.issue_pdu, rpki.up_down.revoke_syntax, and rpki.up_down.message_pdu.

Definition at line 50 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.194 rpki.up_down.certificate_elt Class Reference

Inherits rpki::up_down::base_elt.

Collaboration diagram for rpki.up_down.certificate_elt:

Public Member Functions

- def endElement
- def startElement
- def toXML

Public Attributes

- cert
- cert_url
- req_resource_set_as
- req_resource_set_ipv4
- req_resource_set_ipv6

14.194.1 Detailed Description

```
Up-Down protocol representation of an issued certificate.
```

Definition at line 128 of file up_down.py.

14.194.2 Member Function Documentation

14.194.2.1 def rpki.up_down.certificate_elt.endElement (*self*, *stack*, *name*, *text*)

```
Handle text content of a <certificate/> element.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 143 of file up_down.py.

14.194.2.2 def rpki.up_down.certificate_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle attributes of <certificate/> element.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 133 of file up_down.py.

14.194.2.3 def rpki.up_down.certificate_elt.toXML (*self*)

```
Generate a <certificate/> element.
```

Definition at line 151 of file up_down.py.

14.194.3 Member Data Documentation

14.194.3.1 rpki.up_down.certificate_elt.cert

Definition at line 148 of file up_down.py.

14.194.3.2 rpki.up_down.certificate_elt.cert_url

Definition at line 138 of file up_down.py.

14.194.3.3 rpki.up_down.certificate_elt.req_resource_set_as

Definition at line 139 of file up_down.py.

14.194.3.4 rpki.up_down.certificate_elt.req_resource_set_ipv4

Definition at line 140 of file up_down.py.

14.194.3.5 rpki.up_down.certificate_elt.req_resource_set_ipv6

Definition at line 141 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.195 rpki.up_down.class_elt Class Reference

Inherits rpki::up_down::base_elt.

Collaboration diagram for rpki.up_down.class_elt:

Public Member Functions

- def __init__
- def endElement
- def from_resource_bag
- def startElement
- def to_resource_bag
- def toXML

Public Attributes

- cert_url
- certs
- class_name
- resource_set_as
- resource_set_ipv4
- resource_set_ipv6
- resource_set_notafter
- suggested_sia_head

Static Public Attributes

- issuer = None

14.195.1 Detailed Description

```
Up-Down protocol representation of a resource class.
```

Definition at line 160 of file up_down.py.

14.195.2 Member Function Documentation

14.195.2.1 def rpki.up_down.class_elt.__init__ (*self*)

```
Initialize class_elt.
```

Definition at line 167 of file up_down.py.

14.195.2.2 def rpki.up_down.class_elt.endElement (*self*, *stack*, *name*, *text*)

```
Handle <class/> elements and their children.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 191 of file up_down.py.

14.195.2.3 def rpki.up_down.class_elt.from_resource_bag (*self*, *bag*)

```
Set resources of this class element from a resource_bag.
```

Definition at line 222 of file up_down.py.

14.195.2.4 def rpki.up_down.class_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle <class/> elements and their children.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 172 of file up_down.py.

14.195.2.5 def rpki.up_down.class_elt.to_resource_bag (*self*)

```
Build a resource_bag from from this <class/> element.
```

Definition at line 213 of file up_down.py.

14.195.2.6 def rpki.up_down.class_elt.toXML (*self*)

```
Generate a <class/> element.
```

Definition at line 201 of file up_down.py.

14.195.3 Member Data Documentation

14.195.3.1 rpki.up_down.class_elt.cert_url

Definition at line 184 of file up_down.py.

14.195.3.2 rpki.up_down.class_elt.certs

Definition at line 170 of file up_down.py.

14.195.3.3 rpki.up_down.class_elt.class_name

Definition at line 183 of file up_down.py.

14.195.3.4 rpki.up_down.class_elt.issuer = None [static]

Definition at line 165 of file up_down.py.

14.195.3.5 rpki.up_down.class_elt.resource_set_as

Definition at line 186 of file up_down.py.

14.195.3.6 rpki.up_down.class_elt.resource_set_ipv4

Definition at line 187 of file up_down.py.

14.195.3.7 rpki.up_down.class_elt.resource_set_ipv6

Definition at line 188 of file up_down.py.

14.195.3.8 rpki.up_down.class_elt.resource_set_notafter

Definition at line 189 of file up_down.py.

14.195.3.9 rpki.up_down.class_elt.suggested_sia_head

Definition at line 185 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.196 rpki.up_down.class_response_syntax Class Reference

Inherits rpki::up_down::base_elt.

Inherited by rpki.up_down.issue_response_pdu, and rpki.up_down.list_response_pdu.

Collaboration diagram for rpki.up_down.class_response_syntax:

Public Member Functions

- def __init__
- def startElement
- def toXML

Public Attributes

- classes

14.196.1 Detailed Description

```
Syntax for Up-Down protocol "list_response" and "issue_response" PDUs.
```

Definition at line 285 of file up_down.py.

14.196.2 Member Function Documentation

14.196.2.1 def rpki.up_down.class_response_syntax.__init__ (*self*)

```
Initialize class_response_syntax.
```

Definition at line 290 of file up_down.py.

14.196.2.2 def rpki.up_down.class_response_syntax.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle "list_response" and "issue_response" PDUs.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 297 of file up_down.py.

14.196.2.3 def rpki.up_down.class_response_syntax.toXML (*self*)

```
Generate payload of "list_response" and "issue_response" PDUs.
```

Definition at line 307 of file up_down.py.

14.196.3 Member Data Documentation

14.196.3.1 rpki.up_down.class_response_syntax.classes

Definition at line 295 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.197 rpki.up_down.cms_msg Class Reference

Inherits rpki::x509::XML_CMS_object.

Inherited by rootd.cms_msg.

Collaboration diagram for rpki.up_down.cms_msg:

Static Public Attributes

- string encoding = "UTF-8"
- saxify = sax_handler.saxify
- schema = rpki.relaxng.up_down

14.197.1 Detailed Description

```
Class to hold a CMS-signed up-down PDU.
```

Definition at line 685 of file up_down.py.

14.197.2 Member Data Documentation

14.197.2.1 string rpki.up_down.cms_msg.encoding = "UTF-8" [static]

Definition at line 690 of file up_down.py.

14.197.2.2 rpki.up_down.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented in rootd.cms_msg.

Definition at line 692 of file up_down.py.

14.197.2.3 rpki.up_down.cms_msg.schema = rpki.relaxng.up_down [static]

Definition at line 691 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.198 rpki.up_down.error_response_pdu Class Reference

Inherits rpki::up_down::base_elt.

Collaboration diagram for rpki.up_down.error_response_pdu:

Public Member Functions

- def __init__
- def check_response
- def endElement
- def toXML

Public Attributes

- description
- status

Static Public Attributes

- dictionary codes
- dictionary exceptions

14.198.1 Detailed Description

```
Up-Down protocol "error_response" PDU.
```

Definition at line 505 of file up_down.py.

14.198.2 Member Function Documentation

14.198.2.1 def rpki.up_down.error_response_pdu.__init__ (*self*, *exception* = `None`)

```
Initialize an error_response PDU from an exception object.
```

Definition at line 524 of file up_down.py.

14.198.2.2 def rpki.up_down.error_response_pdu.check_response (*self*)

```
Handle an error response.  For now, just raise an exception,
perhaps figure out something more clever to do later.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 564 of file up_down.py.

14.198.2.3 def rpki.up_down.error_response_pdu.endElement (*self*, *stack*, *name*, *text*)

```
Handle "error_response" PDU.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 533 of file up_down.py.

14.198.2.4 def rpki.up_down.error_response_pdu.toXML (*self*)

```
Generate payload of "error_response" PDU.
```

Definition at line 549 of file up_down.py.

14.198.3 Member Data Documentation

14.198.3.1 dictionary rpki.up_down.error_response_pdu.codes [static]

Initial value:

```
{
    1101 : "Already processing request",
    1102 : "Version number error",
    1103 : "Unrecognised request type",
    1201 : "Request - no such resource class",
    1202 : "Request - no resources allocated in resource class",
    1203 : "Request - badly formed certificate request",
    1301 : "Revoke - no such resource class",
    1302 : "Revoke - no such key",
    2001 : "Internal Server Error - Request not performed" }
```

Definition at line 510 of file up_down.py.

14.198.3.2 rpki.up_down.error_response_pdu.description

Definition at line 531 of file up_down.py.

14.198.3.3 dictionary rpki.up_down.error_response_pdu.exceptions [static]

Initial value:

```
{
    rpki.exceptions.NoActiveCA : 1202 }
```

Definition at line 521 of file up_down.py.

14.198.3.4 rpki.up_down.error_response_pdu.status

Definition at line 530 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.199 rpki.up_down.issue_pdu Class Reference

Inherits rpki::up_down::base_elt.

Inherited by rootd.issue_pdu.

Collaboration diagram for rpki.up_down.issue_pdu:

Public Member Functions

- def endElement
- def query
- def serve_pdu
- def startElement
- def toXML

Public Attributes

- class_name
- pkcs10
- req_resource_set_as
- req_resource_set_ipv4
- req_resource_set_ipv6

14.199.1 Detailed Description

```
Up-Down protocol "issue" PDU.
```

Definition at line 317 of file up_down.py.

14.199.2 Member Function Documentation

14.199.2.1 def rpki.up_down.issue_pdu.endElement (*self*, *stack*, *name*, *text*)

```
Handle "issue" PDU.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 332 of file up_down.py.

14.199.2.2 def rpki.up_down.issue_pdu.query (*cls*, *parent*, *ca*, *ca_detail*, *callback*, *errback*)

```
Send an "issue" request to parent associated with ca.
```

Definition at line 418 of file up_down.py.

14.199.2.3 def rpki.up_down.issue_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *callback*, *errback*)

```
Serve one issue request PDU.
```

Reimplemented from rpki.up_down.base_elt.

Reimplemented in rootd.issue_pdu.

Definition at line 349 of file up_down.py.

14.199.2.4 def rpki.up_down.issue_pdu.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle "issue" PDU.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 322 of file up_down.py.

14.199.2.5 def rpki.up_down.issue_pdu.toXML (*self*)

```
Generate payload of "issue" PDU.
```

Definition at line 340 of file up_down.py.

14.199.3 Member Data Documentation

14.199.3.1 rpki.up_down.issue_pdu.class_name

Definition at line 327 of file up_down.py.

14.199.3.2 rpki.up_down.issue_pdu.pkcs10

Definition at line 337 of file up_down.py.

14.199.3.3 rpki.up_down.issue_pdu.req_resource_set_as

Definition at line 328 of file up_down.py.

14.199.3.4 rpki.up_down.issue_pdu.req_resource_set_ipv4

Definition at line 329 of file up_down.py.

14.199.3.5 rpki.up_down.issue_pdu.req_resource_set_ipv6

Definition at line 330 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.200 rpki.up_down.issue_response_pdu Class Reference

Inherits rpki::up_down::class_response_syntax.

Collaboration diagram for rpki.up_down.issue_response_pdu:

Public Member Functions

- def check_response

14.200.1 Detailed Description

```
Up-Down protocol "issue_response" PDU.
```

Definition at line 431 of file up_down.py.

14.200.2 Member Function Documentation

14.200.2.1 def rpki.up_down.issue_response_pdu.check_response (*self*)

```
Check whether this looks like a reasonable issue_response PDU.
XML schema should be tighter for this response.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 436 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.201 rpki.up_down.list_pdu Class Reference

Inherits rpki::up_down::base_elt.

Inherited by rootd.list_pdu.

Collaboration diagram for rpki.up_down.list_pdu:

Public Member Functions

- def query

- def serve_pdu
- def toXML

14.201.1 Detailed Description

```
Up-Down protocol "list" PDU.
```

Definition at line 231 of file up_down.py.

14.201.2 Member Function Documentation

14.201.2.1 def rpki.up_down.list_pdu.query (*cls*, *parent*, *cb*, *eb*)

```
Send a "list" query to parent.
```

Definition at line 273 of file up_down.py.

14.201.2.2 def rpki.up_down.list_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *callback*, *errback*)

```
Serve one "list" PDU.
```

Reimplemented from rpki.up_down.base_elt.

Reimplemented in rootd.list_pdu.

Definition at line 240 of file up_down.py.

14.201.2.3 def rpki.up_down.list_pdu.toXML (*self*)

```
Generate (empty) payload of "list" PDU.
```

Definition at line 236 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.202 rpki.up_down.list_response_pdu Class Reference

Inherits rpki::up_down::class_response_syntax.

Collaboration diagram for rpki.up_down.list_response_pdu:

14.202.1 Detailed Description

Up-Down protocol "list_response" PDU.

Definition at line 311 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.203 rpki.up_down.message_pdu Class Reference

Inherits rpki::up_down::base_elt.

Inherited by rootd.message_pdu.

Collaboration diagram for rpki.up_down.message_pdu:

Public Member Functions

- def __str__
- def log_query
- def make_query
- def serve_error
- def serve_top_level

- def startElement
- def toXML

Public Attributes

- payload
- recipient
- sender
- type
- version

Static Public Attributes

- dictionary name2type
- tuple type2name = dict((v, k) for k, v in name2type.items())
- int version = 1

14.203.1 Detailed Description

```
Up-Down protocol message wrapper PDU.
```

Definition at line 571 of file up_down.py.

14.203.2 Member Function Documentation

14.203.2.1 def rpki.up_down.message_pdu.__str__ (*self*)

```
Convert a message PDU to a string.
```

Definition at line 613 of file up_down.py.

14.203.2.2 def rpki.up_down.message_pdu.log_query (*self*, *child*)

```
Log query we're handling.  Separate method so rootd can override.
```

Reimplemented in rootd.message_pdu.

Definition at line 642 of file up_down.py.

14.203.2.3 def rpki.up_down.message_pdu.make_query (*cls*, *payload*, *sender*, *recipient*)

```
Construct one message PDU.
```

Definition at line 660 of file up_down.py.

14.203.2.4 def rpki.up_down.message_pdu.serve_error (*self*, *exception*)

```
Generate an error_response message PDU.
```

Definition at line 648 of file up_down.py.

14.203.2.5 def rpki.up_down.message_pdu.serve_top_level (*self*, *child*, *callback*)

```
Serve one message request PDU.
```

Definition at line 617 of file up_down.py.

14.203.2.6 def rpki.up_down.message_pdu.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle message PDU.

Payload of the <message/> element varies depending on the "type"
attribute, so after some basic checks we have to instantiate the
right class object to handle whatever kind of PDU this is.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 597 of file up_down.py.

14.203.2.7 def rpki.up_down.message_pdu.toXML (*self*)

```
Generate payload of message PDU.
```

Definition at line 589 of file up_down.py.

14.203.3 Member Data Documentation

14.203.3.1 dictionary rpki.up_down.message_pdu.name2type [static]

Initial value:

```
{
    "list"            : list_pdu,
    "list_response"   : list_response_pdu,
    "issue"           : issue_pdu,
    "issue_response"  : issue_response_pdu,
    "revoke"          : revoke_pdu,
    "revoke_response" : revoke_response_pdu,
    "error_response"  : error_response_pdu }
```

Reimplemented in rootd.message_pdu.

Definition at line 578 of file up_down.py.

14.203.3.2 rpki.up_down.message_pdu.payload

Definition at line 610 of file up_down.py.

14.203.3.3 rpki.up_down.message_pdu.recipient

Definition at line 608 of file up_down.py.

14.203.3.4 rpki.up_down.message_pdu.sender

Definition at line 607 of file up_down.py.

14.203.3.5 rpki.up_down.message_pdu.type

Definition at line 609 of file up_down.py.

14.203.3.6 tuple rpki.up_down.message_pdu.type2name = dict((v, k) for k, v in name2type.items()) [static]

Reimplemented in rootd.message_pdu.

Definition at line 587 of file up_down.py.

14.203.3.7 rpki.up_down.message_pdu.version

Definition at line 606 of file up_down.py.

14.203.3.8 int rpki.up_down.message_pdu.version = 1 `[static]`

Definition at line 576 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.204 rpki.up_down.multi_uri Class Reference

Inherits list.

Collaboration diagram for rpki.up_down.multi_uri:

Public Member Functions

- def __init__
- def __str__
- def rsync

14.204.1 Detailed Description

```
Container for a set of URIs.
```

Definition at line 95 of file up_down.py.

14.204.2 Member Function Documentation

14.204.2.1 def rpki.up_down.multi_uri.__init__ (*self*, *ini*)

```
Initialize a set of URIs, which includes basic some syntax checking.
```

Definition at line 100 of file up_down.py.

14.204.2.2 def rpki.up_down.multi_uri.__str__ (*self*)

```
Convert a multi_uri back to a string representation.
```

Definition at line 115 of file up_down.py.

14.204.2.3 def rpki.up_down.multi_uri.rsync (*self*)

```
Find first rsync://... URI in self.
```

Definition at line 119 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.205 rpki.up_down.revoke_pdu Class Reference

Inherits rpki::up_down::revoke_syntax.

Inherited by rootd.revoke_pdu.

Collaboration diagram for rpki.up_down.revoke_pdu:

Public Member Functions

- def get_SKI
- def query
- def serve_pdu

Public Attributes

- class_name
- ski

14.205.1 Detailed Description

```
Up-Down protocol "revoke" PDU.
```

Definition at line 458 of file up_down.py.

14.205.2 Member Function Documentation

14.205.2.1 def rpki.up_down.revoke_pdu.get_SKI (*self*)

```
Convert g(SKI) encoding from PDU back to raw SKI.
```

Definition at line 463 of file up_down.py.

14.205.2.2 def rpki.up_down.revoke_pdu.query (*cls*, *ca*, *gski*, *cb*, *eb*)

```
Send a "revoke" request for certificate(s) named by gski to parent associated with ca.
```

Definition at line 487 of file up_down.py.

14.205.2.3 def rpki.up_down.revoke_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *cb*, *eb*)

```
Serve one revoke request PDU.
```

Reimplemented from rpki.up_down.base_elt.

Reimplemented in rootd.revoke_pdu.

Definition at line 467 of file up_down.py.

14.205.3 Member Data Documentation

14.205.3.1 rpki.up_down.revoke_pdu.class_name

Reimplemented from rpki.up_down.revoke_syntax.

Definition at line 493 of file up_down.py.

14.205.3.2 rpki.up_down.revoke_pdu.ski

Reimplemented from rpki.up_down.revoke_syntax.

Definition at line 494 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.206 rpki.up_down.revoke_response_pdu Class Reference

Inherits rpki::up_down::revoke_syntax.

Collaboration diagram for rpki.up_down.revoke_response_pdu:

14.206.1 Detailed Description

```
Up-Down protocol "revoke_response" PDU.
```

Definition at line 498 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.207 rpki.up_down.revoke_syntax Class Reference

Inherits rpki::up_down::base_elt.

Inherited by rpki.up_down.revoke_pdu, and rpki.up_down.revoke_response_pdu.

Collaboration diagram for rpki.up_down.revoke_syntax:

Public Member Functions

- def startElement
- def toXML

Public Attributes

- class_name
- ski

14.207.1 Detailed Description

```
Syntax for Up-Down protocol "revoke" and "revoke_response" PDUs.
```

Definition at line 444 of file up_down.py.

14.207.2 Member Function Documentation

14.207.2.1 def rpki.up_down.revoke_syntax.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle "revoke" PDU.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 449 of file up_down.py.

14.207.2.2 def rpki.up_down.revoke_syntax.toXML (*self*)

```
Generate payload of "revoke" PDU.
```

Definition at line 454 of file up_down.py.

14.207.3 Member Data Documentation

14.207.3.1 rpki.up_down.revoke_syntax.class_name

Reimplemented in rpki.up_down.revoke_pdu.

Definition at line 451 of file up_down.py.

14.207.3.2 rpki.up_down.revoke_syntax.ski

Reimplemented in rpki.up_down.revoke_pdu.

Definition at line 452 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.208 rpki.up_down.sax_handler Class Reference

Inherits rpki::xml_utils::sax_handler.

Inherited by rootd.sax_handler.

Collaboration diagram for rpki.up_down.sax_handler:

Static Public Attributes

- string name = "message"
- pdu = message_pdu
- string version = "1"

14.208.1 Detailed Description

```
SAX handler for Up-Down protocol.
```

Definition at line 676 of file up_down.py.

14.208.2 Member Data Documentation

14.208.2.1 string rpki.up_down.sax_handler.name = "message" [static]

Definition at line 682 of file up_down.py.

14.208.2.2 rpki.up_down.sax_handler.pdu = message_pdu [static]

Reimplemented in rootd.sax_handler.

Definition at line 681 of file up_down.py.

14.208.2.3 string rpki.up_down.sax_handler.version = "1" [static]

Definition at line 683 of file up_down.py.

The documentation for this class was generated from the following file:

- up_down.py (3162)

14.209 rpki.x509.CMS_object Class Reference

Inherits rpki::x509::DER_object.

Inherited by rpki.x509.DER_CMS_object, and rpki.x509.XML_CMS_object.

Collaboration diagram for rpki.x509.CMS_object:

Public Member Functions

- def extract
- def get_content
- def get_DER
- def get_POW
- def set_content

- def sign
- def verify

Public Attributes

- content
- DER

  DER value of this object.

- POW

Static Public Attributes

- debug_cms_certs = False

  Set this to True to log a lot of chatter about CMS certificates.

- dump_on_verify_failure = True

  Set this to True to get dumpasn1 dumps of ASN.1 on CMS verify failures.

- tuple econtent_oid = POWify_OID("id-data")
- tuple formats = ("DER", "POW")

  Formats supported in this object.

- tuple other_clear = ("content",)

  Other attributes that self.clear() should whack.

- tuple pem_converter = PEM_converter("CMS")

  PEM converter for this object.

- print_on_der_error = True

  Set this to True to log alleged DER when we have trouble parsing it, in case it's really a Perl backtrace or something.

- require_crls = False

  Set this to False to make CMS CRLs optional in the cases where we would otherwise require them.

14.209.1 Detailed Description

```
Class to hold a CMS-wrapped object.

CMS-wrapped objects are a little different from the other DER_object
types because the signed object is CMS wrapping inner content that's
also ASN.1, and due to our current minimal support for CMS we can't
just handle this as a pretty composite object.  So, for now anyway,
a CMS_object is the outer CMS wrapped object so that the usual DER
and PEM operations do the obvious things, and the inner content is
handle via separate methods.
```

Definition at line 735 of file x509.py.

14.209.2 Member Function Documentation

14.209.2.1 def rpki.x509.CMS_object.extract (*self*)

```
Extract and store inner content from CMS wrapper without verifying
the CMS.

DANGER WILL ROBINSON!!!

Do not use this method on unvalidated data.  Use the verify()
method instead.

If you don't understand this warning, don't use this method.
```

Definition at line 886 of file x509.py.

14.209.2.2 def rpki.x509.CMS_object.get_content (*self*)

```
Get the inner content of this CMS_object.
```

Definition at line 797 of file x509.py.

14.209.2.3 def rpki.x509.CMS_object.get_DER (*self*)

```
Get the DER value of this CMS_object.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 776 of file x509.py.

14.209.2.4 def rpki.x509.CMS_object.get_POW (*self*)

```
Get the POW value of this CMS_object.
```

Definition at line 788 of file x509.py.

14.209.2.5 def rpki.x509.CMS_object.set_content (*self*, *content*)

```
Set the (inner) content of this CMS_object, clearing the wrapper.
```

Definition at line 805 of file x509.py.

14.209.2.6 def rpki.x509.CMS_object.sign (*self*, *keypair*, *certs*, *crls* = **None**, *no_certs* = **False**)

```
Sign and wrap inner content.
```

Definition at line 914 of file x509.py.

14.209.2.7 def rpki.x509.CMS_object.verify (*self*, *ta*)

```
Verify CMS wrapper and store inner content.
```

Definition at line 812 of file x509.py.

14.209.3 Member Data Documentation

14.209.3.1 rpki.x509.CMS_object.content

Reimplemented in rpki.x509.DER_CMS_object, and rpki.x509.XML_CMS_object.

Definition at line 810 of file x509.py.

14.209.3.2 rpki::x509.CMS_object::debug_cms_certs = False [static]

Set this to True to log a lot of chatter about CMS certificates.

Definition at line 761 of file x509.py.

14.209.3.3 rpki.x509.CMS_object.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 784 of file x509.py.

14.209.3.4 rpki::x509.CMS_object::dump_on_verify_failure = True [static]

Set this to True to get dumpasn1 dumps of ASN.1 on CMS verify failures.

Definition at line 756 of file x509.py.

14.209.3.5 tuple rpki.x509.CMS_object.econtent_oid = POWify_OID("id-data") [static]

Reimplemented in rpki.x509.SignedManifest, rpki.x509.ROA, and rpki.x509.XML_-CMS_object.

Definition at line 750 of file x509.py.

14.209.3.6 tuple rpki.x509.CMS_object.formats = ("DER", "POW") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 748 of file x509.py.

14.209.3.7 tuple rpki.x509.CMS_object.other_clear = ("content",) [static]

Other attributes that self.clear() should whack.

Reimplemented from rpki.x509.DER_object.

Definition at line 749 of file x509.py.

14.209.3.8 tuple rpki.x509.CMS_object.pem_converter = PEM_converter("CMS") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Reimplemented in rpki.x509.SignedManifest, and rpki.x509.ROA.

Definition at line 751 of file x509.py.

14.209.3.9 rpki.x509.CMS_object.POW

Definition at line 794 of file x509.py.

14.209.3.10 rpki::x509.CMS_object::print_on_der_error = True [static]

Set this to True to log alleged DER when we have trouble parsing it, in case it's really a Perl backtrace or something.

Definition at line 774 of file x509.py.

14.209.3.11 rpki::x509.CMS_object::require_crls = False [static]

Set this to False to make CMS CRLs optional in the cases where we would otherwise require them.

Some day this option should go away and CRLs should be uncondtionally mandatory in such cases.

Definition at line 768 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

14.210 rpki.x509.CRL Class Reference

Inherits rpki::x509::DER_object.

Collaboration diagram for rpki.x509.CRL:

Public Member Functions

- def generate
- def get_DER
- def get_POW
- def get_POWpkix
- def getIssuer
- def getNextUpdate
- def getThisUpdate

Public Attributes

- DER

  DER value of this object.

- POW
- POWpkix

Static Public Attributes

- tuple formats = ("DER", "POW", "POWpkix")

  Formats supported in this object.

- tuple pem_converter = PEM_converter("X509 CRL")

  PEM converter for this object.

14.210.1 Detailed Description

```
Class to hold a Certificate Revocation List.
```

Definition at line 1140 of file x509.py.

14.210.2 Member Function Documentation

14.210.2.1 def rpki.x509.CRL.generate (*cls*, *keypair*, *issuer*, *serial*, *thisUpdate*, *nextUpdate*, *revokedCertificates*, *version* = 1, *digestType* = "sha256WithRSAEncryption")

```
Generate a new CRL.
```

Definition at line 1196 of file x509.py.

14.210.2.2 def rpki.x509.CRL.get_DER (*self*)

```
Get the DER value of this CRL.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 1148 of file x509.py.

14.210.2.3 def rpki.x509.CRL.get_POW (*self*)

```
Get the POW value of this CRL.
```

Definition at line 1163 of file x509.py.

14.210.2.4 def rpki.x509.CRL.get_POWpkix (*self*)

```
Get the POW.pkix value of this CRL.
```

Definition at line 1172 of file x509.py.

14.210.2.5 def rpki.x509.CRL.getIssuer (*self*)

```
Get issuer value of this CRL.
```

Definition at line 1191 of file x509.py.

14.210.2.6 def rpki.x509.CRL.getNextUpdate (*self*)

```
Get nextUpdate value from this CRL.
```

Definition at line 1187 of file x509.py.

14.210.2.7 def rpki.x509.CRL.getThisUpdate (*self*)

```
Get thisUpdate value from this CRL.
```

Definition at line 1183 of file x509.py.

14.210.3 Member Data Documentation

14.210.3.1 rpki.x509.CRL.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 1156 of file x509.py.

14.210.3.2 tuple rpki.x509.CRL.formats = ("DER", "POW", "POWpkix") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 1145 of file x509.py.

14.210.3.3 tuple rpki.x509.CRL.pem_converter = PEM_converter("X509 CRL") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 1146 of file x509.py.

14.210.3.4 rpki.x509.CRL.POW

Definition at line 1169 of file x509.py.

14.210.3.5 rpki.x509.CRL.POWpkix

Definition at line 1180 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

14.211 rpki.x509.DeadDrop Class Reference

Inherits object.

Collaboration diagram for rpki.x509.DeadDrop:

Public Member Functions

- def __init__
- def dump

Public Attributes

- maildir
- pid

14.211.1 Detailed Description

```
Dead-drop utility for storing copies of CMS messages for debugging or
audit.  At the moment this uses Maildir mailbox format, as it has
approximately the right properties and a number of useful tools for
manipulating it already exist.
```

Definition at line 1035 of file x509.py.

14.211.2 Member Function Documentation

14.211.2.1 def rpki.x509.DeadDrop.__init__ (*self*, *name*)

Definition at line 1043 of file x509.py.

14.211.2.2 def rpki.x509.DeadDrop.dump (*self*, *obj*)

Definition at line 1047 of file x509.py.

14.211.3 Member Data Documentation

14.211.3.1 rpki.x509.DeadDrop.maildir

Definition at line 1044 of file x509.py.

14.211.3.2 rpki.x509.DeadDrop.pid

Definition at line 1045 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

14.212 rpki.x509.DER_CMS_object Class Reference

Inherits rpki::x509::CMS_object.

Inherited by rpki.x509.ROA, and rpki.x509.SignedManifest.

Collaboration diagram for rpki.x509.DER_CMS_object:

Public Member Functions

- def decode

- def encode

Public Attributes

- content

14.212.1 Detailed Description

```
Class to hold CMS objects with DER-based content.
```

Definition at line 950 of file x509.py.

14.212.2 Member Function Documentation

14.212.2.1 def rpki.x509.DER_CMS_object.decode (*self*, *der*)

```
Decode DER and set inner content.
```

Definition at line 959 of file x509.py.

14.212.2.2 def rpki.x509.DER_CMS_object.encode (*self*)

```
Encode inner content for signing.
```

Definition at line 955 of file x509.py.

14.212.3 Member Data Documentation

14.212.3.1 rpki.x509.DER_CMS_object.content

Reimplemented from rpki.x509.CMS_object.

Definition at line 965 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

14.213 rpki.x509.DER_object Class Reference

Inherits object.

Inherited by rpki.x509.CMS_object, rpki.x509.CRL, rpki.x509.PKCS10, rpki.x509.RSA, rpki.x509.RSApublic, and rpki.x509.X509.

Collaboration diagram for rpki.x509.DER_object:

Public Member Functions

- def __cmp__
- def __init__
- def clear
- def dumpasn1
- def empty
- def from_sql
- def gAKI
- def get_3779resources
- def get_AIA
- def get_aia_uri
- def get_AKI
- def get_Base64
- def get_basicConstraints
- def get_DER
- def get_PEM
- def get_SIA
- def get_sia_directory_uri
- def get_sia_manifest_uri
- def get_SKI
- def gSKI
- def hAKI
- def hSKI
- def is_CA
- def set
- def to_sql

Public Attributes

- DER

  DER value of this object.

Static Public Attributes

- tuple formats = ("DER",)

  Formats supported in this object.

- tuple other_clear = ()

  Other attributes that self.clear() should whack.

- pem_converter = None

  PEM converter for this object.

14.213.1 Detailed Description

```
Virtual class to hold a generic DER object.
```

Definition at line 117 of file x509.py.

14.213.2 Member Function Documentation

14.213.2.1 def rpki.x509.DER_object.__cmp__ (*self*, *other*)

```
Compare two DER-encoded objects.
```

Definition at line 212 of file x509.py.

14.213.2.2 def rpki.x509.DER_object.__init__ (*self*, *kw*)

```
Initialize a DER_object.
```

Definition at line 150 of file x509.py.

14.213.2.3 def rpki.x509.DER_object.clear (*self*)

```
Make this object empty.
```

Definition at line 143 of file x509.py.

14.213.2.4 def rpki.x509.DER_object.dumpasn1 (*self*)

```
Pretty print an ASN.1 DER object using cryptlib dumpasn1 tool.
Use a temporary file rather than popen4() because dumpasn1 uses
seek() when decoding ASN.1 content nested in OCTET STRING values.
```

Definition at line 341 of file x509.py.

14.213.2.5 def rpki.x509.DER_object.empty (*self*)

```
Test whether this object is empty.
```

Definition at line 134 of file x509.py.

14.213.2.6 def rpki.x509.DER_object.from_sql (*cls*, *x*)

```
Convert from SQL storage format.
```

Definition at line 333 of file x509.py.

14.213.2.7 def rpki.x509.DER_object.gAKI (*self*)

```
Calculate g(AKI) for this object.  Only work for subclasses
that implement get_AKI().
```

Definition at line 248 of file x509.py.

14.213.2.8 def rpki.x509.DER_object.get_3779resources (*self*)

```
Get RFC 3779 resources as rpki.resource_set objects.  Only works
for subclasses that support getExtensions().
```

Definition at line 320 of file x509.py.

14.213.2.9 def rpki.x509.DER_object.get_AIA (*self*)

```
Get the SIA extension from this object.  Only works for subclasses
that support getExtension().
```

Definition at line 291 of file x509.py.

14.213.2.10 def rpki.x509.DER_object.get_aia_uri (*self*)

```
Get AIA (id-ad-caIssuers) URI from this object.
Only works for subclasses that support getExtension().
```

Definition at line 298 of file x509.py.

14.213.2.11 def rpki.x509.DER_object.get_AKI (*self*)

```
Get the AKI extension from this object.  Only works for subclasses
that support getExtension().
```

Definition at line 255 of file x509.py.

14.213.2.12 def rpki.x509.DER_object.get_Base64 (*self*)

```
Get the Base64 encoding of the DER value of this object.
```

Definition at line 204 of file x509.py.

14.213.2.13 def rpki.x509.DER_object.get_basicConstraints (*self*)

```
Get the basicConstraints extension from this object.  Only works
for subclasses that support getExtension().
```

Definition at line 305 of file x509.py.

14.213.2.14 def rpki.x509.DER_object.get_DER (*self*)

```
Get the DER value of this object.

Subclasses will almost certainly override this method.
```

Reimplemented in rpki.x509.X509, rpki.x509.PKCS10, rpki.x509.RSA, rpki.x509.RSApublic, rpki.x509.CMS_object, and rpki.x509.CRL.

Definition at line 193 of file x509.py.

14.213.2.15 def rpki.x509.DER_object.get_PEM (*self*)

```
Get the PEM representation of this object.
```

Definition at line 208 of file x509.py.

14.213.2.16 def rpki.x509.DER_object.get_SIA (*self*)

```
Get the SIA extension from this object.  Only works for subclasses
that support getExtension().
```

Definition at line 270 of file x509.py.

14.213.2.17 def rpki.x509.DER_object.get_sia_directory_uri (*self*)

```
Get SIA directory (id-ad-caRepository) URI from this object.
Only works for subclasses that support getExtension().
```

Definition at line 277 of file x509.py.

14.213.2.18 def rpki.x509.DER_object.get_sia_manifest_uri (*self*)

```
Get SIA manifest (id-ad-rpkiManifest) URI from this object.
Only works for subclasses that support getExtension().
```

Definition at line 284 of file x509.py.

14.213.2.19 def rpki.x509.DER_object.get_SKI (*self*)

```
Get the SKI extension from this object.  Only works for subclasses
that support getExtension().
```

Reimplemented in rpki.x509.RSA, and rpki.x509.RSApublic.

Definition at line 263 of file x509.py.

14.213.2.20 def rpki.x509.DER_object.gSKI (*self*)

```
Calculate g(SKI) for this object.  Only work for subclasses
that implement get_SKI().
```

Definition at line 233 of file x509.py.

14.213.2.21 def rpki.x509.DER_object.hAKI (*self*)

```
Return hexadecimal string representation of AKI for this
object.  Only work for subclasses that implement get_AKI().
```

Definition at line 240 of file x509.py.

14.213.2.22 def rpki.x509.DER_object.hSKI (*self*)

```
Return hexadecimal string representation of SKI for this object.
Only work for subclasses that implement get_SKI().
```

Definition at line 225 of file x509.py.

14.213.2.23 def rpki.x509.DER_object.is_CA (*self*)

```
Return True if and only if object has the basicConstraints
extension and its cA value is true.
```

Definition at line 312 of file x509.py.

14.213.2.24 def rpki.x509.DER_object.set (*self*, *kw*)

```
Set this object by setting one of its known formats.

This method only allows one to set one format at a time.
Subsequent calls will clear the object first.  The point of all
this is to let the object's internal converters handle mustering
the object into whatever format you need at the moment.
```

Definition at line 158 of file x509.py.

14.213.2.25 def rpki.x509.DER_object.to_sql (*self*)

```
Convert to SQL storage format.
```

Definition at line 337 of file x509.py.

14.213.3 Member Data Documentation

14.213.3.1 rpki::x509.DER_object::DER

DER value of this object.

Reimplemented in rpki.x509.X509, rpki.x509.PKCS10, rpki.x509.RSA, rpki.x509.RSApublic, rpki.x509.CMS_object, and rpki.x509.CRL.

Definition at line 176 of file x509.py.

14.213.3.2 tuple rpki.x509.DER_object.formats = ("DER",) [static]

Formats supported in this object.

Reimplemented in rpki.x509.X509, rpki.x509.PKCS10, rpki.x509.RSA, rpki.x509.RSApublic, rpki.x509.CMS_object, and rpki.x509.CRL.

Definition at line 123 of file x509.py.

14.213.3.3 tuple rpki.x509.DER_object.other_clear = () [static]

Other attributes that self.clear() should whack.

Reimplemented in rpki.x509.CMS_object.

Definition at line 129 of file x509.py.

14.213.3.4 rpki.x509.DER_object.pem_converter = None [static]

PEM converter for this object.

Reimplemented in rpki.x509.X509, rpki.x509.PKCS10, rpki.x509.RSA, rpki.x509.RSApublic, rpki.x509.CMS_object, rpki.x509.SignedManifest, rpki.x509.ROA, and rpki.x509.CRL.

Definition at line 126 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

14.214 rpki.x509.PEM_converter Class Reference

Inherits object.

Collaboration diagram for rpki.x509.PEM_converter:

Public Member Functions

- def __init__
- def looks_like_PEM
- def to_DER

- def to_PEM

Public Attributes

- b
- e

14.214.1 Detailed Description

```
Convert between DER and PEM encodings for various kinds of ASN.1 data.
```

Definition at line 62 of file x509.py.

14.214.2 Member Function Documentation

14.214.2.1 def rpki.x509.PEM_converter.__init__ (*self*, *kind*)

```
Initialize PEM_converter.
```

Definition at line 67 of file x509.py.

14.214.2.2 def rpki.x509.PEM_converter.looks_like_PEM (*self*, *text*)

```
Guess whether text looks like a PEM encoding.
```

Definition at line 74 of file x509.py.

14.214.2.3 def rpki.x509.PEM_converter.to_DER (*self*, *pem*)

```
Convert from PEM to DER.
```

Definition at line 81 of file x509.py.

14.214.2.4 def rpki.x509.PEM_converter.to_PEM (*self*, *der*)

```
Convert from DER to PEM.
```

Definition at line 94 of file x509.py.

14.214.3 Member Data Documentation

14.214.3.1 rpki.x509.PEM_converter.b

Definition at line 71 of file x509.py.

14.214.3.2 rpki.x509.PEM_converter.e

Definition at line 72 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

14.215 rpki.x509.PKCS10 Class Reference

Inherits rpki::x509::DER_object.

Collaboration diagram for rpki.x509.PKCS10:

Public Member Functions

- def check_valid_rpki
- def create
- def create_ca
- def get_DER
- def get_POWpkix
- def getPublicKey

Public Attributes

- DER

  DER value of this object.

- POWpkix

Static Public Attributes

- tuple formats = ("DER", "POWpkix")

  Formats supported in this object.

- tuple pem_converter = PEM_converter("CERTIFICATE REQUEST")

  PEM converter for this object.

14.215.1 Detailed Description

```
Class to hold a PKCS #10 request.
```

Definition at line 534 of file x509.py.

14.215.2 Member Function Documentation

14.215.2.1 def rpki.x509.PKCS10.check_valid_rpki (*self*)

```
Check this certification request to see whether it's a valid
request for an RPKI certificate.  This is broken out of the
up-down protocol code because it's somewhat involved and the
up-down code doesn't need to know the details.

Throws an exception if the request isn't valid, so if this method
returns at all, the request is ok.
```

Definition at line 569 of file x509.py.

14.215.2.2 def rpki.x509.PKCS10.create (*cls*, *keypair*, *exts* = `None`)

```
Create a new request for a given keypair, including given extensions.
```

Definition at line 629 of file x509.py.

14.215.2.3 def rpki.x509.PKCS10.create_ca (*cls*, *keypair*, *sia* = `None`)

```
Create a new request for a given keypair, including given SIA value.
```

Definition at line 616 of file x509.py.

14.215.2.4 def rpki.x509.PKCS10.get_DER (*self*)

```
Get the DER value of this certification request.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 542 of file x509.py.

14.215.2.5 def rpki.x509.PKCS10.get_POWpkix (*self*)

```
Get the POW.pkix value of this certification request.
```

Definition at line 554 of file x509.py.

14.215.2.6 def rpki.x509.PKCS10.getPublicKey (*self*)

```
Extract the public key from this certification request.
```

Definition at line 565 of file x509.py.

14.215.3 Member Data Documentation

14.215.3.1 rpki.x509.PKCS10.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 550 of file x509.py.

14.215.3.2 tuple rpki.x509.PKCS10.formats = ("DER", "POWpkix") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 539 of file x509.py.

14.215.3.3 tuple rpki.x509.PKCS10.pem_converter = PEM_converter("CERTIFICATE REQUEST") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 540 of file x509.py.

14.215.3.4 rpki.x509.PKCS10.POWpkix

Definition at line 562 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

14.216 rpki.x509.ROA Class Reference

Inherits rpki::x509::DER_CMS_object.

Collaboration diagram for rpki.x509.ROA:

Public Member Functions

- def build

Static Public Attributes

- content_class = rpki.roa.RouteOriginAttestation

- tuple econtent_oid = POWify_OID("id-ct-routeOriginAttestation")
- tuple pem_converter = PEM_converter("ROUTE ORIGIN ATTESTATION")

  PEM converter for this object.

14.216.1 Detailed Description

```
Class to hold a signed ROA.
```

Definition at line 1007 of file x509.py.

14.216.2 Member Function Documentation

14.216.2.1 def rpki.x509.ROA.build (*cls*, *asn*, *ipv4*, *ipv6*, *keypair*, *certs*, *version* = 0)

```
Build a ROA.
```

Definition at line 1017 of file x509.py.

14.216.3 Member Data Documentation

14.216.3.1 rpki.x509.ROA.content_class = rpki.roa.RouteOriginAttestation [static]

Definition at line 1013 of file x509.py.

14.216.3.2 tuple rpki.x509.ROA.econtent_oid = POWify_OID("id-ct-routeOriginAttestation") [static]

Reimplemented from rpki.x509.CMS_object.

Definition at line 1014 of file x509.py.

14.216.3.3 tuple rpki.x509.ROA.pem_converter = PEM_converter("ROUTE ORIGIN ATTESTATION") [static]

PEM converter for this object.

Reimplemented from rpki.x509.CMS_object.

Definition at line 1012 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

14.217 rpki.x509.RSA Class Reference

Inherits rpki::x509::DER_object.

Collaboration diagram for rpki.x509.RSA:

Public Member Functions

- def generate
- def get_DER
- def get_POW
- def get_public_DER
- def get_RSApublic
- def get_SKI

Public Attributes

- DER

  DER value of this object.

- POW

Static Public Attributes

- tuple formats = ("DER", "POW")

  Formats supported in this object.

- tuple pem_converter = PEM_converter("RSA PRIVATE KEY")

  PEM converter for this object.

14.217.1 Detailed Description

```
Class to hold an RSA key pair.
```

Definition at line 643 of file x509.py.

14.217.2 Member Function Documentation

14.217.2.1 def rpki.x509.RSA.generate (*cls*, *keylength* = 2048)

```
Generate a new keypair.
```

Definition at line 673 of file x509.py.

14.217.2.2 def rpki.x509.RSA.get_DER (*self*)

```
Get the DER value of this keypair.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 651 of file x509.py.

14.217.2.3 def rpki.x509.RSA.get_POW (*self*)

```
Get the POW value of this keypair.
```

Definition at line 663 of file x509.py.

14.217.2.4 def rpki.x509.RSA.get_public_DER (*self*)

```
Get the DER encoding of the public key from this keypair.
```

Definition at line 680 of file x509.py.

14.217.2.5 def rpki.x509.RSA.get_RSApublic (*self*)

```
Convert the public key of this keypair into a RSApublic object.
```

Definition at line 688 of file x509.py.

14.217.2.6 def rpki.x509.RSA.get_SKI (*self*)

```
Calculate the SKI of this keypair.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 684 of file x509.py.

14.217.3 Member Data Documentation

14.217.3.1 rpki.x509.RSA.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 659 of file x509.py.

14.217.3.2 tuple rpki.x509.RSA.formats = ("DER", "POW") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 648 of file x509.py.

14.217.3.3 tuple rpki.x509.RSA.pem_converter = PEM_converter("RSA PRIVATE KEY") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 649 of file x509.py.

14.217.3.4 rpki.x509.RSA.POW

Definition at line 669 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

14.218 rpki.x509.RSApublic Class Reference

Inherits rpki::x509::DER_object.

Collaboration diagram for rpki.x509.RSApublic:

Public Member Functions

- def get_DER
- def get_POW
- def get_SKI

Public Attributes

- DER

  DER value of this object.

- POW

Static Public Attributes

- tuple formats = ("DER", "POW")

  Formats supported in this object.

- tuple pem_converter = PEM_converter("RSA PUBLIC KEY")

  PEM converter for this object.

14.218.1 Detailed Description

```
Class to hold an RSA public key.
```

Definition at line 692 of file x509.py.

14.218.2 Member Function Documentation

14.218.2.1 def rpki.x509.RSApublic.get_DER (*self*)

```
Get the DER value of this public key.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 700 of file x509.py.

14.218.2.2 def rpki.x509.RSApublic.get_POW (*self*)

```
Get the POW value of this public key.
```

Definition at line 712 of file x509.py.

14.218.2.3 def rpki.x509.RSApublic.get_SKI (*self*)

```
Calculate the SKI of this public key.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 721 of file x509.py.

14.218.3 Member Data Documentation

14.218.3.1 rpki.x509.RSApublic.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 708 of file x509.py.

14.218.3.2 tuple rpki.x509.RSApublic.formats = ("DER", "POW") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 697 of file x509.py.

14.218.3.3 tuple rpki.x509.RSApublic.pem_converter = PEM_converter("RSA PUBLIC KEY") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 698 of file x509.py.

14.218.3.4 rpki.x509.RSApublic.POW

Definition at line 718 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

14.219 rpki.x509.SignedManifest Class Reference

Inherits rpki::x509::DER_CMS_object.

Collaboration diagram for rpki.x509.SignedManifest:

Public Member Functions

- def build
- def getNextUpdate
- def getThisUpdate

Static Public Attributes

- content_class = rpki.manifest.Manifest
- tuple econtent_oid = POWify_OID("id-ct-rpkiManifest")
- tuple pem_converter = PEM_converter("RPKI MANIFEST")

  PEM converter for this object.

14.219.1 Detailed Description

```
Class to hold a signed manifest.
```

Definition at line 967 of file x509.py.

14.219.2 Member Function Documentation

14.219.2.1 def rpki.x509.SignedManifest.build (*cls*, *serial*, *thisUpdate*, *nextUpdate*, *names_and_objs*, *keypair*, *certs*, *version* = 0)

```
Build a signed manifest.
```

Definition at line 985 of file x509.py.

14.219.2.2 def rpki.x509.SignedManifest.getNextUpdate (*self*)

```
Get nextUpdate value from this manifest.
```

Definition at line 980 of file x509.py.

14.219.2.3 def rpki.x509.SignedManifest.getThisUpdate (*self*)

```
Get thisUpdate value from this manifest.
```

Definition at line 976 of file x509.py.

14.219.3 Member Data Documentation

14.219.3.1 rpki.x509.SignedManifest.content_class = rpki.manifest.Manifest [static]

Definition at line 973 of file x509.py.

14.219.3.2 tuple rpki.x509.SignedManifest.econtent_oid = POWify_OID("id-ct-rpkiManifest") [static]

Reimplemented from rpki.x509.CMS_object.

Definition at line 974 of file x509.py.

14.219.3.3 tuple rpki.x509.SignedManifest.pem_converter = PEM_converter("RPKI MANIFEST") [static]

PEM converter for this object.

Reimplemented from rpki.x509.CMS_object.

Definition at line 972 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

14.220 rpki.x509.X509 Class Reference

Inherits rpki::x509::DER_object.

Collaboration diagram for rpki.x509.X509:

Public Member Functions

- def cross_certify
- def expired
- def get_DER
- def get_POW
- def get_POWpkix

- def getIssuer
- def getNotAfter
- def getNotBefore
- def getPublicKey
- def getSerial
- def getSubject
- def issue
- def normalize_chain

Public Attributes

- DER

  DER value of this object.

- POW
- POWpkix

Static Public Attributes

- tuple formats = ("DER", "POW", "POWpkix")

  Formats supported in this object.

- tuple pem_converter = PEM_converter("CERTIFICATE")

  PEM converter for this object.

14.220.1 Detailed Description

```
X.509 certificates.

This class is designed to hold all the different representations of
X.509 certs we're using and convert between them.  X.509 support in
Python a nasty maze of half-cooked stuff (except perhaps for
cryptlib, which is just different).  Users of this module should not
have to care about this implementation nightmare.
```

Definition at line 360 of file x509.py.

14.220.2 Member Function Documentation

14.220.2.1 def rpki.x509.X509.cross_certify (*self*, *keypair*, *source_cert*, *serial*, *notAfter*, *now* = `None`, *pathLenConstraint* = `0`)

```
Issue a certificate with values taking from an existing certificate.
This is used to construct some kinds oF BPKI certificates.
```

Definition at line 492 of file x509.py.

14.220.2.2 def rpki.x509.X509.expired (*self*)

```
Test whether this certificate has expired.
```

Definition at line 433 of file x509.py.

14.220.2.3 def rpki.x509.X509.get_DER (*self*)

```
Get the DER value of this certificate.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 374 of file x509.py.

14.220.2.4 def rpki.x509.X509.get_POW (*self*)

```
Get the POW value of this certificate.
```

Definition at line 389 of file x509.py.

14.220.2.5 def rpki.x509.X509.get_POWpkix (*self*)

```
Get the POW.pkix value of this certificate.
```

Definition at line 398 of file x509.py.

14.220.2.6 def rpki.x509.X509.getIssuer (*self*)

```
Get the issuer of this certificate.
```

Definition at line 409 of file x509.py.

14.220.2.7 def rpki.x509.X509.getNotAfter (*self*)

```
Get the expiration time of this certificate.
```

Definition at line 421 of file x509.py.

14.220.2.8 def rpki.x509.X509.getNotBefore (*self*)

```
Get the inception time of this certificate.
```

Definition at line 417 of file x509.py.

14.220.2.9 def rpki.x509.X509.getPublicKey (*self*)

```
Extract the public key from this certificate.
```

Definition at line 429 of file x509.py.

14.220.2.10 def rpki.x509.X509.getSerial (*self*)

```
Get the serial number of this certificate.
```

Definition at line 425 of file x509.py.

14.220.2.11 def rpki.x509.X509.getSubject (*self*)

```
Get the subject of this certificate.
```

Definition at line 413 of file x509.py.

14.220.2.12 def rpki.x509.X509.issue (*self*, *keypair*, *subject_key*, *serial*, *sia*, *aia*, *crldp*, *notAfter*, *cn* = `None`, *resources* = `None`, *is_ca* = `True`)

```
Issue a certificate.
```

Definition at line 437 of file x509.py.

14.220.2.13 def rpki.x509.X509.normalize_chain (*cls*, *chain*)

```
Normalize a chain of certificates into a tuple of X509 objects.
Given all the glue certificates needed for BPKI cross
certification, it's easiest to allow sloppy arguments to the HTTPS
and CMS validation methods and provide a single method that
normalizes the allowed cases.  So this method allows X509, None,
lists, and tuples, and returns a tuple of X509 objects.
```

Definition at line 521 of file x509.py.

14.220.3 Member Data Documentation

14.220.3.1 rpki.x509.X509.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 382 of file x509.py.

14.220.3.2 tuple rpki.x509.X509.formats = ("DER", "POW", "POWpkix") `[static]`

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 371 of file x509.py.

14.220.3.3 tuple rpki.x509.X509.pem_converter = PEM_converter("CERTIFICATE") `[static]`

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 372 of file x509.py.

14.220.3.4 rpki.x509.X509.POW

Definition at line 395 of file x509.py.

14.220.3.5 rpki.x509.X509.POWpkix

Definition at line 406 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

14.221 rpki.x509.XML_CMS_object Class Reference

Inherits rpki::x509::CMS_object.

Inherited by rpki.left_right.cms_msg, rpki.publication.cms_msg, and rpki.up_-down.cms_msg.

Collaboration diagram for rpki.x509.XML_CMS_object:

Public Member Functions

- def decode
- def dump_to_disk
- def encode
- def pretty_print_content
- def schema_check

- def unwrap
- def wrap

Public Attributes

- content

Static Public Attributes

- dump_inbound_cms = None

  If set, we write all inbound XML-CMS PDUs to disk, for debugging.

- dump_outbound_cms = None

  If set, we write all outbound XML-CMS PDUs to disk, for debugging.

- tuple econtent_oid = POWify_OID("id-ct-xml")

14.221.1 Detailed Description

```
Class to hold CMS-wrapped XML protocol data.
```

Definition at line 1058 of file x509.py.

14.221.2 Member Function Documentation

14.221.2.1 def rpki.x509.XML_CMS_object.decode (*self*, *xml*)

```
Decode XML and set inner content.
```

Definition at line 1081 of file x509.py.

14.221.2.2 def rpki.x509.XML_CMS_object.dump_to_disk (*self*, *prefix*)

```
Write DER of current message to disk, for debugging.
```

Definition at line 1099 of file x509.py.

14.221.2.3 def rpki.x509.XML_CMS_object.encode (*self*)

```
Encode inner content for signing.
```

Definition at line 1077 of file x509.py.

14.221.2.4 def rpki.x509.XML_CMS_object.pretty_print_content (*self*)

```
Pretty print XML content of this message.
```

Definition at line 1085 of file x509.py.

14.221.2.5 def rpki.x509.XML_CMS_object.schema_check (*self*)

```
Handle XML RelaxNG schema check.
```

Definition at line 1089 of file x509.py.

14.221.2.6 def rpki.x509.XML_CMS_object.unwrap (*cls*, *der*, *ta*, *pretty_print* = `False`)

```
Unwrap a CMS-wrapped XML PDU and return Python objects.
```

Definition at line 1125 of file x509.py.

14.221.2.7 def rpki.x509.XML_CMS_object.wrap (*cls*, *msg*, *keypair*, *certs*, *crls* = `None`, *pretty_print* = `False`)

```
Build a CMS-wrapped XML PDU and return its DER encoding.
```

Definition at line 1108 of file x509.py.

14.221.3 Member Data Documentation

14.221.3.1 rpki.x509.XML_CMS_object.content

Reimplemented from rpki.x509.CMS_object.

Definition at line 1083 of file x509.py.

14.221.3.2 rpki::x509.XML_CMS_object::dump_inbound_cms = None [static]

If set, we write all inbound XML-CMS PDUs to disk, for debugging.

If set, value should be a DeadDrop object.

Definition at line 1075 of file x509.py.

14.221.3.3 rpki::x509.XML_CMS_object::dump_outbound_cms = None [static]

If set, we write all outbound XML-CMS PDUs to disk, for debugging.

If set, value should be a DeadDrop object.

Definition at line 1069 of file x509.py.

14.221.3.4 tuple rpki.x509.XML_CMS_object.econtent_oid = POWify_OID("id-ct-xml") [static]

Reimplemented from rpki.x509.CMS_object.

Definition at line 1063 of file x509.py.

The documentation for this class was generated from the following file:

- x509.py (3107)

14.222 rpki.xml_utils.base_elt Class Reference

Inherits object.

Inherited by rpki.left_right.list_received_resources_elt, rpki.left_right.list_resources_-elt, rpki.left_right.list_roa_requests_elt, rpki.publication.publication_object_elt, rpki.xml_utils.data_elt, and rpki.xml_utils.text_elt.

Collaboration diagram for rpki.xml_utils.base_elt:

Public Member Functions

- def __str__
- def endElement

- def make_b64elt
- def make_elt
- def make_pdu
- def read_attrs
- def startElement
- def toXML

Static Public Attributes

- tuple attributes = ()

  XML attributes for this element.

- tuple booleans = ()

  Boolean attributes (value "yes" or "no") for this element.

- tuple elements = ()

  XML elements contained by this element.

14.222.1 Detailed Description

```
Virtual base class for XML message elements.  The left-right and
publication protocols use this.  At least for now, the up-down
protocol does not, due to different design assumptions.
```

Definition at line 126 of file xml_utils.py.

14.222.2 Member Function Documentation

14.222.2.1 def rpki.xml_utils.base_elt.__str__ (*self*)

```
Convert a base_elt object to string format.
```

Reimplemented in rpki.publication.report_error_elt.

Definition at line 201 of file xml_utils.py.

14.222.2.2 def rpki.xml_utils.base_elt.endElement (*self*, *stack*, *name*, *text*)

```
Default endElement() handler: just pop the stack.
```

Reimplemented in rpki.left_right.child_elt, rpki.publication.client_elt, rpki.publication.publication_object_elt, rpki.xml_utils.text_elt, and rpki.xml_-utils.data_elt.

Definition at line 153 of file xml_utils.py.

14.222.2.3 def rpki.xml_utils.base_elt.make_b64elt (*self*, *elt*, *name*, *value* = `None`)

```
Constructor for Base64-encoded subelement.
```

Definition at line 192 of file xml_utils.py.

14.222.2.4 def rpki.xml_utils.base_elt.make_elt (*self*)

```
XML element constructor.
```

Definition at line 178 of file xml_utils.py.

14.222.2.5 def rpki.xml_utils.base_elt.make_pdu (*cls*, *kargs*)

```
Generic PDU constructor.
```

Definition at line 208 of file xml_utils.py.

14.222.2.6 def rpki.xml_utils.base_elt.read_attrs (*self*, *attrs*)

```
Template-driven attribute reader.
```

Definition at line 166 of file xml_utils.py.

14.222.2.7 def rpki.xml_utils.base_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Default startElement() handler: just process attributes.
```

Reimplemented in rpki.left_right.list_resources_elt, rpki.left_right.list_roa_requests_-elt, and rpki.publication.config_elt.

Definition at line 145 of file xml_utils.py.

14.222.2.8 def rpki.xml_utils.base_elt.toXML (*self*)

```
Default toXML() element generator.
```

Reimplemented in rpki.left_right.list_resources_elt, rpki.publication.publication_-object_elt, rpki.xml_utils.text_elt, and rpki.xml_utils.data_elt.

Definition at line 160 of file xml_utils.py.

14.222.3 Member Data Documentation

14.222.3.1 rpki::xml_utils.base_elt::attributes = () [static]

XML attributes for this element.

Reimplemented in rpki.left_right.self_elt, rpki.left_right.bsc_elt, rpki.left_-right.repository_elt, rpki.left_right.parent_elt, rpki.left_right.child_elt, rpki.left_-right.list_resources_elt, rpki.left_right.list_roa_requests_elt, rpki.left_right.list_-published_objects_elt, rpki.left_right.list_received_resources_elt, rpki.left_-right.report_error_elt, rpki.publication.config_elt, rpki.publication.client_elt, rpki.publication.publication_object_elt, and rpki.publication.report_error_elt.

Definition at line 135 of file xml_utils.py.

14.222.3.2 rpki::xml_utils.base_elt::booleans = () [static]

Boolean attributes (value "yes" or "no") for this element.

Reimplemented in rpki.left_right.self_elt, rpki.left_right.bsc_elt, rpki.left_-right.parent_elt, and rpki.left_right.child_elt.

Definition at line 143 of file xml_utils.py.

14.222.3.3 rpki::xml_utils.base_elt::elements = () [static]

XML elements contained by this element.

Reimplemented in rpki.left_right.self_elt, rpki.left_right.bsc_elt, rpki.left_-right.repository_elt, rpki.left_right.parent_elt, rpki.left_right.child_elt, rpki.publication.config_elt, and rpki.publication.client_elt.

Definition at line 139 of file xml_utils.py.

The documentation for this class was generated from the following file:

- xml_utils.py (2836)

14.223 rpki.xml_utils.data_elt Class Reference

Inherits rpki::xml_utils::base_elt.

Inherited by rpki.left_right.data_elt, and rpki.publication.control_elt.

Collaboration diagram for rpki.xml_utils.data_elt:

Public Member Functions

- def endElement
- def make_reply
- def make_reply_clone_hook
- def serve_create
- def serve_destroy

- def serve_destroy_hook
- def serve_dispatch
- def serve_fetch_one
- def serve_get
- def serve_list
- def serve_post_save_hook
- def serve_pre_save_hook
- def serve_set
- def toXML
- def unimplemented_control

14.223.1 Detailed Description

```
Virtual base class for PDUs that map to SQL objects.  These objects
all implement the create/set/get/list/destroy action attribute.
```

Definition at line 243 of file xml_utils.py.

14.223.2 Member Function Documentation

14.223.2.1 def rpki.xml_utils.data_elt.endElement (*self*, *stack*, *name*, *text*)

```
Default endElement handler for SQL-based objects.  This assumes
that sub-elements are Base64-encoded using the sql_template
mechanism.
```

Reimplemented from rpki.xml_utils.base_elt.

Reimplemented in rpki.left_right.child_elt, and rpki.publication.client_elt.

Definition at line 249 of file xml_utils.py.

14.223.2.2 def rpki.xml_utils.data_elt.make_reply (*self*, *r_pdu* = `None`)

```
Construct a reply PDU.
```

Definition at line 275 of file xml_utils.py.

14.223.2.3 def rpki.xml_utils.data_elt.make_reply_clone_hook (*self*, *r_pdu*)

```
Overridable hook.
```

Reimplemented in rpki.left_right.data_elt.

Definition at line 292 of file xml_utils.py.

14.223.2.4 def rpki.xml_utils.data_elt.serve_create (*self*, *r_msg*, *cb*, *eb*)

```
Handle a create action.
```

Definition at line 314 of file xml_utils.py.

14.223.2.5 def rpki.xml_utils.data_elt.serve_destroy (*self*, *r_msg*, *cb*, *eb*)

```
Handle a destroy action.
```

Definition at line 384 of file xml_utils.py.

14.223.2.6 def rpki.xml_utils.data_elt.serve_destroy_hook (*self*, *cb*, *eb*)

```
Overridable hook.
```

Reimplemented in rpki.left_right.child_elt.

Definition at line 378 of file xml_utils.py.

14.223.2.7 def rpki.xml_utils.data_elt.serve_dispatch (*self*, *r_msg*, *cb*, *eb*)

```
Action dispatch handler.
```

Reimplemented in rpki.publication.control_elt.

Definition at line 395 of file xml_utils.py.

14.223.2.8 def rpki.xml_utils.data_elt.serve_fetch_one (*self*)

```
Find the object on which a get, set, or destroy method should
operate.
```

Definition at line 296 of file xml_utils.py.

14.223.2.9 def rpki.xml_utils.data_elt.serve_get (*self*, *r_msg*, *cb*, *eb*)

```
Handle a get action.
```

Definition at line 360 of file xml_utils.py.

14.223.2.10 def rpki.xml_utils.data_elt.serve_list (*self*, *r_msg*, *cb*, *eb*)

```
Handle a list action for non-self objects.
```

Definition at line 369 of file xml_utils.py.

14.223.2.11 def rpki.xml_utils.data_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Overridable hook.
```

Reimplemented in rpki.left_right.self_elt, rpki.left_right.parent_elt, rpki.left_-right.child_elt, and rpki.publication.client_elt.

Definition at line 310 of file xml_utils.py.

14.223.2.12 def rpki.xml_utils.data_elt.serve_pre_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

```
Overridable hook.
```

Reimplemented in rpki.left_right.data_elt, and rpki.left_right.bsc_elt.

Definition at line 306 of file xml_utils.py.

14.223.2.13 def rpki.xml_utils.data_elt.serve_set (*self*, *r_msg*, *cb*, *eb*)

```
Handle a set action.
```

Reimplemented in rpki.publication.config_elt.

Definition at line 337 of file xml_utils.py.

14.223.2.14 def rpki.xml_utils.data_elt.toXML (*self*)

```
Default element generator for SQL-based objects.  This assumes
that sub-elements are Base64-encoded DER objects.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 263 of file xml_utils.py.

14.223.2.15 def rpki.xml_utils.data_elt.unimplemented_control (*self*, *controls*)

```
Uniform handling for unimplemented control operations.
```

Definition at line 408 of file xml_utils.py.

The documentation for this class was generated from the following file:

- xml_utils.py (2836)

14.224 rpki.xml_utils.msg Class Reference

Inherits list.

Inherited by rpki.left_right.msg, and rpki.publication.msg.

Collaboration diagram for rpki.xml_utils.msg:

Public Member Functions

- def __str__
- def endElement
- def is_query
- def is_reply
- def query
- def reply
- def startElement
- def toXML

Public Attributes

- type
- version

14.224.1 Detailed Description

```
Generic top-level PDU.
```

Definition at line 416 of file xml_utils.py.

14.224.2 Member Function Documentation

14.224.2.1 def rpki.xml_utils.msg.__str__ (*self*)

```
Convert msg object to string.
```

Definition at line 442 of file xml_utils.py.

14.224.2.2 def rpki.xml_utils.msg.endElement (*self*, *stack*, *name*, *text*)

```
Handle top-level PDU.
```

Definition at line 434 of file xml_utils.py.

14.224.2.3 def rpki.xml_utils.msg.is_query (*self*)

```
Is this msg a query?
```

Definition at line 468 of file xml_utils.py.

14.224.2.4 def rpki.xml_utils.msg.is_reply (*self*)

```
Is this msg a reply?
```

Definition at line 472 of file xml_utils.py.

14.224.2.5 def rpki.xml_utils.msg.query (*cls*, *args*)

```
Create a query PDU.
```

Definition at line 455 of file xml_utils.py.

14.224.2.6 def rpki.xml_utils.msg.reply (*cls*, *args*)

```
Create a reply PDU.
```

Definition at line 462 of file xml_utils.py.

14.224.2.7 def rpki.xml_utils.msg.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle top-level PDU.
```

Definition at line 421 of file xml_utils.py.

14.224.2.8 def rpki.xml_utils.msg.toXML (*self*)

```
Generate top-level PDU.
```

Definition at line 446 of file xml_utils.py.

14.224.3 Member Data Documentation

14.224.3.1 rpki.xml_utils.msg.type

Definition at line 427 of file xml_utils.py.

14.224.3.2 rpki.xml_utils.msg.version

Reimplemented in rpki.left_right.msg, and rpki.publication.msg.

Definition at line 426 of file xml_utils.py.

The documentation for this class was generated from the following file:

- xml_utils.py (2836)

14.225 rpki.xml_utils.sax_handler Class Reference

Inherits xml::sax::handler::ContentHandler.

Inherited by rpki.left_right.sax_handler, rpki.publication.sax_handler, and rpki.up_-down.sax_handler.

Collaboration diagram for rpki.xml_utils.sax_handler:

Public Member Functions

- def __init__
- def characters
- def create_top_level
- def endElement
- def endElementNS
- def saxify
- def startElement
- def startElementNS

Public Attributes

- result
- stack
- text

14.225.1 Detailed Description

```
SAX handler for RPKI protocols.

This class provides some basic amenities for parsing protocol XML of
the kind we use in the RPKI protocols, including whacking all the
protocol element text into US-ASCII, simplifying accumulation of
text fields, and hiding some of the fun relating to XML namespaces.

General assumption: by the time this parsing code gets invoked, the
XML has already passed RelaxNG validation, so we only have to check
for errors that the schema can't catch, and we don't have to play as
many XML namespace games.
```

Definition at line 38 of file xml_utils.py.

14.225.2 Member Function Documentation

14.225.2.1 def rpki.xml_utils.sax_handler.__init__ (*self*)

```
Initialize SAX handler.
```

Definition at line 53 of file xml_utils.py.

14.225.2.2 def rpki.xml_utils.sax_handler.characters (*self*, *content*)

```
Accumulate a chuck of element content (text).
```

Definition at line 69 of file xml_utils.py.

14.225.2.3 def rpki.xml_utils.sax_handler.create_top_level (*self*, *name*, *attrs*)

```
Handle top-level PDU for this protocol.
```

Definition at line 119 of file xml_utils.py.

14.225.2.4 def rpki.xml_utils.sax_handler.endElement (*self*, *name*)

```
Handle endElement() events.  Mostly this means handling any
accumulated element text.
```

Definition at line 101 of file xml_utils.py.

14.225.2.5 def rpki.xml_utils.sax_handler.endElementNS (*self*, *name*, *qname*)

```
Redirect endElementNS() events to endElement().
```

Definition at line 65 of file xml_utils.py.

14.225.2.6 def rpki.xml_utils.sax_handler.saxify (*cls*, *elt*)

```
Create a one-off SAX parser, parse an ETree, return the result.
```

Definition at line 111 of file xml_utils.py.

14.225.2.7 def rpki.xml_utils.sax_handler.startElement (*self*, *name*, *attrs*)

```
Handle startElement() events.

We maintain a stack of nested elements under construction so that
we can feed events directly to the current element rather than
having to pass them through all the nesting elements.

If the stack is empty, this event is for the outermost element, so
we call a virtual method to create the corresponding object and
that's the object we'll be returning as our final result.
```

Definition at line 73 of file xml_utils.py.

14.225.2.8 def rpki.xml_utils.sax_handler.startElementNS (*self*, *name*, *qname*, *attrs*)

```
Redirect startElementNS() events to startElement().
```

Definition at line 61 of file xml_utils.py.

14.225.3 Member Data Documentation

14.225.3.1 rpki.xml_utils.sax_handler.result

Definition at line 97 of file xml_utils.py.

14.225.3.2 rpki.xml_utils.sax_handler.stack

Definition at line 59 of file xml_utils.py.

14.225.3.3 rpki.xml_utils.sax_handler.text

Definition at line 58 of file xml_utils.py.

The documentation for this class was generated from the following file:

- xml_utils.py (2836)

14.226 rpki.xml_utils.text_elt Class Reference

Inherits rpki::xml_utils::base_elt.

Inherited by rpki.left_right.list_published_objects_elt, rpki.left_right.report_error_elt, and rpki.publication.report_error_elt.

Collaboration diagram for rpki.xml_utils.text_elt:

Public Member Functions

- def endElement
- def toXML

Static Public Attributes

- text_attribute = None

  Name of the class attribute that holds the text value.

14.226.1 Detailed Description

```
Virtual base class for XML message elements that contain text.
```

Definition at line 219 of file xml_utils.py.

14.226.2 Member Function Documentation

14.226.2.1 def rpki.xml_utils.text_elt.endElement (*self*, *stack*, *name*, *text*)

```
Extract text from parsed XML.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 228 of file xml_utils.py.

14.226.2.2 def rpki.xml_utils.text_elt.toXML (*self*)

```
Insert text into generated XML.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 235 of file xml_utils.py.

14.226.3 Member Data Documentation

14.226.3.1 rpki::xml_utils.text_elt::text_attribute = None [static]

Name of the class attribute that holds the text value.

Reimplemented in rpki.left_right.list_published_objects_elt, rpki.left_right.report_-error_elt, and rpki.publication.report_error_elt.

Definition at line 226 of file xml_utils.py.

The documentation for this class was generated from the following file:

- xml_utils.py (2836)

14.227 Sequence Class Reference

Inherited by rpki.manifest.FileAndHash, rpki.manifest.Manifest, rpki.roa.ROAIPAddress, rpki.roa.ROAIPAddressFamily, and rpki.roa.RouteOriginAttestation.

The documentation for this class was generated from the following file:

- roa.py (2424)

14.228 SequenceOf Class Reference

Inherited by rpki.manifest.FilesAndHashes, rpki.roa.ROAIPAddresses, and rpki.roa.ROAIPAddressFamilies.

The documentation for this class was generated from the following file:

- roa.py (2424)

14.229 set Class Reference

Inherited by rpki.myrpki.comma_set.

The documentation for this class was generated from the following file:

- myrpki.py

14.230 TextWrapper Class Reference

Inherited by irbe_cli.UsageWrapper.

The documentation for this class was generated from the following file:

- irbe_cli.py (3107)

14.231 ContentHandler Class Reference

Inherited by rpki.xml_utils.sax_handler.

The documentation for this class was generated from the following file:

- xml_utils.py (2836)

15 File Documentation

15.1 __doc__.py File Reference

Packages

- package rpki.__doc__

15.1.1 Detailed Description

Documentation sourc, expressed as Python comments to make Doxygen happy.

Id

__doc__.py.in 3214 2010-04-19 16:36:33Z sra

Copyright (C) 2009-2010 Internet Systems Consortium ("ISC")

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Portions copyright (C) 2007--2008 American Registry for Internet Numbers ("ARIN")

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED

WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ARIN BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Definition in file __doc__.py.

15.2 __init__.py File Reference

Packages

- package rpki

15.3 async.py File Reference

Classes

- class rpki.async.gc_summary
- class rpki.async.iterator
- class rpki.async.sync_wrapper
- class rpki.async.timer

Packages

- package rpki.async

Functions

- def rpki::async._raiseExitNow
- def rpki::async.defer
- def rpki::async.event_loop
- def rpki::async.exit_event_loop
- def rpki::async.run_deferred

Variables

- list rpki::async.deferred_queue = [ ]

  List to hold deferred actions.

- rpki::async.ExitNow = asyncore.ExitNow

15.4 cli.py File Reference

Classes

- class rpki.cli.Cmd

Packages

- package rpki.cli

Functions

- def rpki::cli.yes_or_no

Variables

- dictionary rpki::cli._yes_or_no_prompts
- rpki::cli.have_readline = True

15.5 config.py File Reference

Classes

- class rpki.config.parser

Packages

- package rpki.config

15.6 exceptions.py File Reference

Classes

- class rpki.exceptions.BadClassNameSyntax
- class rpki.exceptions.BadClientURL
- class rpki.exceptions.BadContactURL
- class rpki.exceptions.BadExtension
- class rpki.exceptions.BadIRDBReply
- class rpki.exceptions.BadIssueResponse
- class rpki.exceptions.BadPKCS10
- class rpki.exceptions.BadPublicationReply

- class rpki.exceptions.BadQuery
- class rpki.exceptions.BadSender
- class rpki.exceptions.BadStatusCode
- class rpki.exceptions.BadURISyntax
- class rpki.exceptions.BSCNotFound
- class rpki.exceptions.BSCNotReady
- class rpki.exceptions.ChildNotFound
- class rpki.exceptions.ClassNameMismatch
- class rpki.exceptions.ClassNameUnknown
- class rpki.exceptions.ClientNotFound
- class rpki.exceptions.CMSContentNotSet
- class rpki.exceptions.CMSCRLNotSet
- class rpki.exceptions.CMSVerificationFailed
- class rpki.exceptions.DBConsistancyError
- class rpki.exceptions.DERObjectConversionError
- class rpki.exceptions.DuplicateObject
- class rpki.exceptions.EmptyPEM
- class rpki.exceptions.EmptyROAPrefixList
- class rpki.exceptions.ForbiddenURI
- class rpki.exceptions.HandleTranslationError
- class rpki.exceptions.HTTPRequestFailed
- class rpki.exceptions.HTTPSBadVersion
- class rpki.exceptions.HTTPSClientAborted
- class rpki.exceptions.HTTPSUnexpectedState
- class rpki.exceptions.MissingCMSCRL
- class rpki.exceptions.MissingCMSEEcert
- class rpki.exceptions.MultipleTLSEECert
- class rpki.exceptions.MustBePrefix
- class rpki.exceptions.NoActiveCA
- class rpki.exceptions.NoCoveringCertForROA
- class rpki.exceptions.NoObjectAtURI
- class rpki.exceptions.NotACertificateChain
- class rpki.exceptions.NotFound
- class rpki.exceptions.NotImplementedYet
- class rpki.exceptions.NotInDatabase
- class rpki.exceptions.ReceivedTLSCACert
- class rpki.exceptions.RPKI_Exception
- class rpki.exceptions.ServerShuttingDown
- class rpki.exceptions.SKIMismatch
- class rpki.exceptions.SubprocessError
- class rpki.exceptions.TLSValidationError
- class rpki.exceptions.UnexpectedCMSCerts
- class rpki.exceptions.UnexpectedCMSCRLs

- class rpki.exceptions.UnparsableCMSDER
- class rpki.exceptions.UpstreamError
- class rpki.exceptions.WrongEContentType

Packages

- package rpki.exceptions

15.7 https.py File Reference

Classes

- class rpki.https.caller
- class rpki.https.http_client
- class rpki.https.http_listener
- class rpki.https.http_message
- class rpki.https.http_queue
- class rpki.https.http_request
- class rpki.https.http_response
- class rpki.https.http_server
- class rpki.https.http_stream

Packages

- package rpki.https

Functions

- def rpki::https.build_https_ta_cache
- def rpki::https.client
- def rpki::https.log_method
- def rpki::https.server

Variables

- dictionary rpki::https.client_queues = { }

  Map of (host, port) tuples to http_queue objects.

- rpki::https.debug_http = False

  Verbose chatter about HTTP streams.

- rpki::https.debug_tls_certs = False

  Verbose chatter about TLS certificates.

- tuple rpki::https.default_client_timeout = rpki.sundial.timedelta(minutes = 15)

  Default HTTP client connection timeout.

- tuple rpki::https.default_http_version = (1, 0)

  Preferred HTTP version.

- tuple rpki::https.default_server_timeout = rpki.sundial.timedelta(minutes = 20)

  Default HTTP server connection timeouts.

- string rpki::https.rpki_content_type = "application/x-rpki"

  HTTP content type used for all RPKI messages.

- tuple rpki::https.supported_address_families = (socket.AF_INET, socket.AF_INET6)

  IP address families to support.

- rpki::https.want_persistent_client = False

  Whether we want persistent HTTP client streams, when server also supports them.

- rpki::https.want_persistent_server = False

  Whether we want persistent HTTP server streams, when client also supports them.

15.8 ipaddrs.py File Reference

Classes

- class rpki.ipaddrs.v4addr
- class rpki.ipaddrs.v6addr

Packages

- package rpki.ipaddrs

15.9 irbe_cli.py File Reference

Classes

- class irbe_cli.bsc_elt
- class irbe_cli.certificate_elt
- class irbe_cli.child_elt
- class irbe_cli.client_elt
- class irbe_cli.cmd_elt_mixin
- class irbe_cli.cmd_msg_mixin
- class irbe_cli.config_elt
- class irbe_cli.crl_elt
- class irbe_cli.left_right_cms_msg
- class irbe_cli.left_right_msg
- class irbe_cli.left_right_proto
- class irbe_cli.left_right_sax_handler
- class irbe_cli.list_published_objects_elt
- class irbe_cli.list_received_resources_elt
- class irbe_cli.manifest_elt
- class irbe_cli.parent_elt
- class irbe_cli.publication_cms_msg
- class irbe_cli.publication_msg
- class irbe_cli.publication_proto
- class irbe_cli.publication_sax_handler
- class irbe_cli.reply_elt_mixin
- class irbe_cli.report_error_elt
- class irbe_cli.report_error_elt
- class irbe_cli.repository_elt
- class irbe_cli.roa_elt
- class irbe_cli.self_elt
- class irbe_cli.UsageWrapper

Packages

- package irbe_cli

Functions

- def irbe_cli.usage

Variables

- list irbe_cli.argv = sys.argv[1:]
- tuple irbe_cli.call_pubd
- tuple irbe_cli.call_rpkid
- tuple irbe_cli.cfg = rpki.config.parser(cfg_file, "irbe_cli")
- string irbe_cli.cfg_file = "irbe.conf"
- irbe_cli.pem_out = None
- irbe_cli.q_msg = q_msg_left_right
- list irbe_cli.q_msg_left_right = [ ]
- list irbe_cli.q_msg_publication = [ ]
- list irbe_cli.q_pdu = left_right_msg.pdus[argv[0]]
- list irbe_cli.top_opts = ["config=", "help", "pem_out=", "quiet", "verbose"]
- tuple irbe_cli.usage_fill = UsageWrapper(subsequent_indent = " " ∗ 4)
- irbe_cli.verbose = True

15.10 irdbd.py File Reference

Packages

- package irdbd

Functions

- def irdbd.handle_list_resources
- def irdbd.handle_list_roa_requests
- def irdbd.handler

Variables

- tuple irdbd.bpki_ta = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))
- tuple irdbd.cfg = rpki.config.parser(cfg_file, "irdbd")
- string irdbd.cfg_file = "irdbd.conf"
- tuple irdbd.client_ta = (bpki_ta, rpkid_cert)
- tuple irdbd.cur = db.cursor()
- tuple irdbd.db
- dictionary irdbd.handle_dispatch
- tuple irdbd.handlers = ((u.path, handler),)
- string irdbd.host = "localhost"
- tuple irdbd.irdbd_cert = rpki.x509.X509(Auto_file = cfg.get("irdbd-cert"))
- tuple irdbd.irdbd_key = rpki.x509.RSA(Auto_file = cfg.get("irdbd-key"))
- int irdbd.port = 443

- tuple irdbd.rpkid_cert = rpki.x509.X509(Auto_file = cfg.get("rpkid-cert"))
- irdbd.server_cert = irdbd_cert,
- tuple irdbd.startup_msg = cfg.get("startup-message", "")
- tuple irdbd.u = urlparse.urlparse(cfg.get("https-url"))

15.11 left_right.py File Reference

Classes

- class rpki.left_right.bsc_elt
- class rpki.left_right.child_elt
- class rpki.left_right.cms_msg
- class rpki.left_right.data_elt
- class rpki.left_right.left_right_namespace
- class rpki.left_right.list_published_objects_elt
- class rpki.left_right.list_received_resources_elt
- class rpki.left_right.list_resources_elt
- class rpki.left_right.list_roa_requests_elt
- class rpki.left_right.msg
- class rpki.left_right.parent_elt
- class rpki.left_right.report_error_elt
- class rpki.left_right.repository_elt
- class rpki.left_right.sax_handler
- class rpki.left_right.self_elt

Packages

- package rpki.left_right

Variables

- rpki::left_right.enforce_strict_up_down_xml_sender = False

15.12 log.py File Reference

Classes

- class rpki.log.logger

Packages

- package rpki.log

Functions

- def rpki::log.init
- def rpki::log.set_trace
- def rpki::log.trace
- def rpki::log.traceback

Variables

- tuple rpki::log.debug = logger(syslog.LOG_DEBUG)
- rpki::log.enable_trace = False

  Whether call tracing is enabled.

- tuple rpki::log.error = logger(syslog.LOG_ERR)
- tuple rpki::log.info = logger(syslog.LOG_INFO)
- tuple rpki::log.note = logger(syslog.LOG_NOTICE)
- int rpki::log.pid = 0
- string rpki::log.tag = ""
- rpki::log.use_syslog = True

  Whether to use syslog.

- tuple rpki::log.warn = logger(syslog.LOG_WARNING)

15.13 manifest.py File Reference

Classes

- class rpki.manifest.FileAndHash
- class rpki.manifest.FilesAndHashes
- class rpki.manifest.Manifest

Packages

- package rpki.manifest

15.14 myrpki.py File Reference

Classes

- class rpki.myrpki.CA
- class rpki.myrpki.child
- class rpki.myrpki.children

- class rpki.myrpki.comma_set
- class rpki.myrpki.csv_reader
- class rpki.myrpki.EntityDB
- class rpki.myrpki.main
- class rpki.myrpki.parent
- class rpki.myrpki.parents
- class rpki.myrpki.repositories
- class rpki.myrpki.repository
- class rpki.myrpki.roa_request
- class rpki.myrpki.roa_requests

Packages

- package rpki.myrpki

Functions

- def rpki::myrpki.b64_equal
- def rpki::myrpki.csv_writer
- def rpki::myrpki.etree_post_read
- def rpki::myrpki.etree_pre_write
- def rpki::myrpki.etree_read
- def rpki::myrpki.etree_validate
- def rpki::myrpki.etree_write
- def rpki::myrpki.PEMElement

Variables

- rpki::myrpki.allow_incomplete = False
- string rpki::myrpki.namespace = "http://www.hactrn.net/uris/rpki/myrpki/"
- string rpki::myrpki.namespaceQName = "{"
- string rpki::myrpki.version = "2"
- rpki::myrpki.whine = False

15.15 oids.py File Reference

Packages

- package rpki.oids

Variables

- tuple rpki::oids.name2oid = dict((v, k) for k, v in oid2name.items())

  Mapping table of string names to OIDs.

- dictionary rpki::oids.oid2name

  Mapping table of OIDs to conventional string names.

15.16 pubd.py File Reference

Classes

- class pubd.pubd_context

Packages

- package pubd

Functions

- def pubd.main

Variables

- string pubd.cfg_file = "pubd.conf"
- pubd.profile = False

15.17 publication.py File Reference

Classes

- class rpki.publication.certificate_elt
- class rpki.publication.client_elt
- class rpki.publication.cms_msg
- class rpki.publication.config_elt
- class rpki.publication.control_elt
- class rpki.publication.crl_elt
- class rpki.publication.manifest_elt
- class rpki.publication.msg
- class rpki.publication.publication_namespace

- class rpki.publication.publication_object_elt
- class rpki.publication.report_error_elt
- class rpki.publication.roa_elt
- class rpki.publication.sax_handler

Packages

- package rpki.publication

15.18 relaxng.py File Reference

Packages

- package rpki.relaxng

Variables

- tuple rpki::relaxng.left_right

  Parsed RelaxNG left_right schema.

- tuple rpki::relaxng.publication

  Parsed RelaxNG publication schema.

- tuple rpki::relaxng.up_down

  Parsed RelaxNG up_down schema.

15.19 resource_set.py File Reference

Classes

- class rpki.resource_set.resource_bag
- class rpki.resource_set.resource_range
- class rpki.resource_set.resource_range_as
- class rpki.resource_set.resource_range_ip
- class rpki.resource_set.resource_range_ipv4
- class rpki.resource_set.resource_range_ipv6
- class rpki.resource_set.resource_set
- class rpki.resource_set.resource_set_as
- class rpki.resource_set.resource_set_ip
- class rpki.resource_set.resource_set_ipv4

- class rpki.resource_set.resource_set_ipv6
- class rpki.resource_set.roa_prefix
- class rpki.resource_set.roa_prefix_ipv4
- class rpki.resource_set.roa_prefix_ipv6
- class rpki.resource_set.roa_prefix_set
- class rpki.resource_set.roa_prefix_set_ipv4
- class rpki.resource_set.roa_prefix_set_ipv6

Packages

- package rpki.resource_set

Functions

- def rpki::resource_set._bs2long
- def rpki::resource_set._long2bs
- def rpki::resource_set._rsplit
- def rpki::resource_set.test1
- def rpki::resource_set.test2

Variables

- string rpki::resource_set.inherit_token = "<inherit>"

  Token used to indicate inheritance in read and print syntax.

15.20 roa.py File Reference

Classes

- class rpki.roa.ROAIPAddress
- class rpki.roa.ROAIPAddresses
- class rpki.roa.ROAIPAddressFamilies
- class rpki.roa.ROAIPAddressFamily
- class rpki.roa.RouteOriginAttestation

Packages

- package rpki.roa

15.21 rootd.py File Reference

Classes

- class rootd.cms_msg
- class rootd.issue_pdu
- class rootd.list_pdu
- class rootd.message_pdu
- class rootd.revoke_pdu
- class rootd.sax_handler

Packages

- package rootd

Functions

- def rootd.compose_response
- def rootd.del_subject_cert
- def rootd.del_subject_pkcs10
- def rootd.get_root_cert
- def rootd.get_subject_cert
- def rootd.get_subject_pkcs10
- def rootd.issue_subject_cert_maybe
- def rootd.root_newer_than_subject
- def rootd.set_subject_cert
- def rootd.set_subject_pkcs10
- def rootd.up_down_handler

Variables

- tuple rootd.bpki_ta = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))
- tuple rootd.cfg = rpki.config.parser(cfg_file, "rootd")
- string rootd.cfg_file = "rootd.conf"
- tuple rootd.child_bpki_cert = rpki.x509.X509(Auto_file = cfg.get("child-bpki-cert"))
- tuple rootd.client_ta = (bpki_ta, child_bpki_cert)
- rootd.handlers = up_down_handler)
- rootd.host = https_server_host,
- tuple rootd.https_server_host = cfg.get("server-host", "")
- tuple rootd.https_server_port = int(cfg.get("server-port"))
- rootd.port = https_server_port,

- tuple rootd.rootd_bpki_cert = rpki.x509.X509(Auto_file = cfg.get("rootd-bpki-cert"))
- tuple rootd.rootd_bpki_crl = rpki.x509.CRL(Auto_file = cfg.get("rootd-bpki-crl"))
- tuple rootd.rootd_bpki_key = rpki.x509.RSA(Auto_file = cfg.get("rootd-bpki-key"))
- tuple rootd.rpki_base_uri = cfg.get("rpki-base-uri", "rsync://" + rpki_class_name + ".invalid/")
- tuple rootd.rpki_class_name = cfg.get("rpki-class-name", "wombat")
- rootd.rpki_root_cert = None
- tuple rootd.rpki_root_cert_file = cfg.get("rpki-root-cert")
- tuple rootd.rpki_root_cert_uri = cfg.get("rpki-root-cert-uri", rpki_base_uri + "Root.cer")
- tuple rootd.rpki_root_crl = cfg.get("rpki-root-crl", "Root.crl")
- tuple rootd.rpki_root_dir = cfg.get("rpki-root-dir")
- tuple rootd.rpki_root_key = rpki.x509.RSA(Auto_file = cfg.get("rpki-root-key"))
- tuple rootd.rpki_root_manifest = cfg.get("rpki-root-manifest", "Root.mnf")
- tuple rootd.rpki_subject_cert = cfg.get("rpki-subject-cert", "Child.cer")
- tuple rootd.rpki_subject_lifetime = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-lifetime", "30d"))
- tuple rootd.rpki_subject_pkcs10 = cfg.get("rpki-subject-pkcs10", "Child.pkcs10")
- tuple rootd.rpki_subject_regen = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-regen", rpki_subject_lifetime.convert_to_seconds() / 2))
- rootd.server_cert = rootd_bpki_cert,

15.22 rpki_engine.py File Reference

Classes

- class rpki.rpki_engine.ca_detail_obj
- class rpki.rpki_engine.ca_obj
- class rpki.rpki_engine.child_cert_obj
- class rpki.rpki_engine.publication_queue
- class rpki.rpki_engine.revoked_cert_obj
- class rpki.rpki_engine.roa_obj
- class rpki.rpki_engine.rpkid_context

Packages

- package rpki.rpki_engine

15.23 rpkid.py File Reference

Packages

- package rpkid

Functions

- def rpkid.main

Variables

- string rpkid.cfg_file = "rpkid.conf"
- rpkid.profile = None

15.24 sql.py File Reference

Classes

- class rpki.sql.session
- class rpki.sql.sql_persistent
- class rpki.sql.template

Packages

- package rpki.sql

15.25 sundial.py File Reference

Classes

- class rpki.sundial.datetime
- class rpki.sundial.timedelta

Packages

- package rpki.sundial

Functions

- def rpki::sundial._cast
- def rpki::sundial.now
- def rpki::sundial.test

15.26 up_down.py File Reference

Classes

- class rpki.up_down.base_elt
- class rpki.up_down.certificate_elt
- class rpki.up_down.class_elt
- class rpki.up_down.class_response_syntax
- class rpki.up_down.cms_msg
- class rpki.up_down.error_response_pdu
- class rpki.up_down.issue_pdu
- class rpki.up_down.issue_response_pdu
- class rpki.up_down.list_pdu
- class rpki.up_down.list_response_pdu
- class rpki.up_down.message_pdu
- class rpki.up_down.multi_uri
- class rpki.up_down.revoke_pdu
- class rpki.up_down.revoke_response_pdu
- class rpki.up_down.revoke_syntax
- class rpki.up_down.sax_handler

Packages

- package rpki.up_down

Variables

- dictionary rpki::up_down.nsmap = { None : xmlns }
- string rpki::up_down.xmlns = "http://www.apnic.net/specs/rescerts/up-down/"

15.27 x509.py File Reference

Classes

- class rpki.x509.CMS_object
- class rpki.x509.CRL

- class rpki.x509.DeadDrop
- class rpki.x509.DER_CMS_object
- class rpki.x509.DER_object
- class rpki.x509.PEM_converter
- class rpki.x509.PKCS10
- class rpki.x509.ROA
- class rpki.x509.RSA
- class rpki.x509.RSApublic
- class rpki.x509.SignedManifest
- class rpki.x509.X509
- class rpki.x509.XML_CMS_object

Packages

- package rpki.x509

Functions

- def rpki::x509._find_xia_uri
- def rpki::x509.calculate_SKI
- def rpki::x509.POWify_OID

15.28 xml_utils.py File Reference

Classes

- class rpki.xml_utils.base_elt
- class rpki.xml_utils.data_elt
- class rpki.xml_utils.msg
- class rpki.xml_utils.sax_handler
- class rpki.xml_utils.text_elt

Packages

- package rpki.xml_utils

Index

__abs__
  rpki::sundial::timedelta, 571
__add__
  rpki::sundial::datetime, 564
  rpki::sundial::timedelta, 571
__call__
  irbe_cli::UsageWrapper, 166
  rpki::async::iterator, 186
  rpki::async::sync_wrapper, 190
  rpki::https::caller, 265
  rpki::log::logger, 367
  rpki::myrpki::EntityDB, 392
__cmp__
  rpki::async::timer, 194
  rpki::resource_set::resource_range, 457
  rpki::resource_set::roa_prefix, 483
  rpki::x509::DER_object, 635
__del__
  rpki::async::timer, 194
__div__
  rpki::sundial::timedelta, 571
__doc__.py, 691
__eq__
  rpki::resource_set::resource_bag, 453
__floordiv__
  rpki::sundial::timedelta, 571
__init__
  pubd::pubd_context, 168
  rpki::async::gc_summary, 184
  rpki::async::iterator, 186
  rpki::async::sync_wrapper, 190
  rpki::async::timer, 194
  rpki::cli::Cmd, 199
  rpki::config::parser, 204
  rpki::https::caller, 265
  rpki::https::http_client, 268
  rpki::https::http_listener, 274
  rpki::https::http_message, 277
  rpki::https::http_queue, 281
  rpki::https::http_request, 285
  rpki::https::http_response, 288
  rpki::https::http_server, 291
  rpki::https::http_stream, 297
  rpki::log::logger, 367
  rpki::manifest::FileAndHash, 369
  rpki::manifest::FilesAndHashes, 370
  rpki::manifest::Manifest, 372
  rpki::myrpki::CA, 375
  rpki::myrpki::child, 382
  rpki::myrpki::csv_reader, 389
  rpki::myrpki::EntityDB, 392
  rpki::myrpki::main, 394
  rpki::myrpki::parent, 401
  rpki::myrpki::repository, 408
  rpki::myrpki::roa_request, 411
  rpki::resource_set::resource_bag, 453
  rpki::resource_set::resource_range, 457
  rpki::resource_set::resource_set, 469
  rpki::resource_set::roa_prefix, 483
  rpki::resource_set::roa_prefix_set, 491
  rpki::roa::ROAIPAddress, 497
  rpki::roa::ROAIPAddresses, 499
  rpki::roa::ROAIPAddressFamilies, 500
  rpki::roa::ROAIPAddressFamily, 501
  rpki::roa::RouteOriginAttestation, 503
  rpki::rpki_engine::child_cert_obj, 522
  rpki::rpki_engine::publication_-queue, 527
  rpki::rpki_engine::revoked_cert_obj, 530
  rpki::rpki_engine::roa_obj, 534
  rpki::rpki_engine::rpkid_context, 542
  rpki::sql::session, 549
  rpki::sql::template, 561

rpki::up_down::class_elt, 581
rpki::up_down::class_response_-syntax, 585
rpki::up_down::error_response_pdu, 590
rpki::up_down::multi_uri, 608
rpki::x509::DeadDrop, 630
rpki::x509::DER_object, 635
rpki::x509::PEM_converter, 642
rpki::xml_utils::sax_handler, 685
__init__.py(3150), 692
__iter__
rpki::myrpki::csv_reader, 389
__mul__
rpki::sundial::timedelta, 571
__ne__
rpki::resource_set::resource_bag, 453
__neg__
rpki::sundial::timedelta, 571
__new__
rpki::ipaddrs::v4addr, 304
rpki::ipaddrs::v6addr, 307
__pos__
rpki::sundial::timedelta, 571
__radd__
rpki::sundial::datetime, 564
rpki::sundial::timedelta, 571
__rdiv__
rpki::sundial::timedelta, 572
__repr__
rpki::async::iterator, 187
rpki::async::timer, 194
rpki::myrpki::child, 382
rpki::myrpki::parent, 401
rpki::myrpki::repository, 408
rpki::myrpki::roa_request, 411
__rfloordiv__
rpki::sundial::timedelta, 572
__rmul__
rpki::sundial::timedelta, 572
__rsub__
rpki::sundial::datetime, 564
rpki::sundial::timedelta, 572
__str__
rpki::https::http_message, 277
rpki::ipaddrs::v4addr, 304
rpki::ipaddrs::v6addr, 307
rpki::myrpki::comma_set, 387
rpki::publication::report_error_elt, 445
rpki::resource_set::resource_bag, 454
rpki::resource_set::resource_range_-as, 459
rpki::resource_set::resource_range_-ip, 462
rpki::resource_set::resource_set, 469
rpki::resource_set::roa_prefix, 483
rpki::resource_set::roa_prefix_set, 491
rpki::sundial::datetime, 565
rpki::up_down::message_pdu, 604
rpki::up_down::multi_uri, 609
rpki::xml_utils::base_elt, 672
rpki::xml_utils::msg, 682
__sub__
rpki::sundial::datetime, 565
rpki::sundial::timedelta, 572
_add
rpki::rpki_engine::publication_-queue, 527
_bs2long
rpki::resource_set, 103
_cast
rpki::sundial, 108
_comm
rpki::resource_set::resource_set, 469
_exceptions_enabled
rpki::sql::session, 550
_find_xia_uri
rpki::x509, 112
_long2bs
rpki::resource_set, 103
_prefixlen
rpki::resource_set::resource_range_-ip, 462
_raiseExitNow
rpki::async, 77
_regexp
rpki::config::parser, 206
_repl

rpki::config::parser, 204
_rsplit
rpki::resource_set, 104
_wrap_execute
rpki::sql::session, 549
_yes_or_no_prompts
rpki::cli, 80

activate
rpki::rpki_engine::ca_detail_obj, 507
add
rpki::myrpki::child, 382
rpki::myrpki::children, 385
rpki::myrpki::parent, 401
rpki::myrpki::parents, 403
rpki::myrpki::repositories, 405
rpki::myrpki::repository, 408
rpki::myrpki::roa_request, 411
rpki::myrpki::roa_requests, 413
address
rpki::roa::ROAIPAddress, 498
addresses
rpki::roa::ROAIPAddressFamily, 502
addressFamily
rpki::roa::ROAIPAddressFamily, 502
af
rpki::https::http_client, 271
afi
rpki::resource_set::resource_set_-ipv4, 479
rpki::resource_set::resource_set_-ipv6, 481
allow_incomplete
rpki::myrpki, 97
argv
irbe_cli, 60
asID
rpki::roa::RouteOriginAttestation, 503
asn
rpki::left_right::list_resources_elt, 335
rpki::myrpki::roa_request, 412
rpki::resource_set::resource_bag, 455
rpki::rpki_engine::roa_obj, 537
asns
rpki::myrpki::child, 383
assert_pristine
rpki::sql::session, 549
async.py(3191), 692
asynchat::async_chat, 115
asyncore::dispatcher, 115
attributes
rpki::left_right::bsc_elt, 311
rpki::left_right::child_elt, 317
rpki::left_right::list_published_-objects_elt, 329
rpki::left_right::list_received_-resources_elt, 331
rpki::left_right::list_resources_elt, 335
rpki::left_right::list_roa_requests_-elt, 337
rpki::left_right::parent_elt, 345
rpki::left_right::report_error_elt, 350
rpki::left_right::repository_elt, 354
rpki::left_right::self_elt, 364
rpki::publication::client_elt, 419
rpki::publication::config_elt, 426
rpki::publication::publication_-object_elt, 442
rpki::publication::report_error_elt, 446
rpki::xml_utils::base_elt, 674

b
rpki::x509::PEM_converter, 643
b64_equal
rpki::myrpki, 96
base_uri
rpki::publication::client_elt, 419
bits
rpki::ipaddrs::v4addr, 305
rpki::ipaddrs::v6addr, 307
body
rpki::https::http_message, 279
booleans
rpki::left_right::bsc_elt, 311

rpki::left_right::child_elt, 317
rpki::left_right::parent_elt, 345
rpki::left_right::self_elt, 364
rpki::xml_utils::base_elt, 674
bpki_cert
irbe_cli::cmd_elt_mixin, 129
rpki::left_right::child_elt, 317
rpki::left_right::repository_elt, 354
rpki::left_right::self_elt, 364
rpki::publication::client_elt, 420
bpki_certificate
rpki::myrpki::child, 383
rpki::myrpki::repository, 408
bpki_cms_cert
irbe_cli::cmd_elt_mixin, 129
rpki::left_right::parent_elt, 345
bpki_cms_certificate
rpki::myrpki::parent, 402
bpki_cms_glue
irbe_cli::cmd_elt_mixin, 129
rpki::left_right::parent_elt, 345
bpki_crl
irbe_cli::config_elt, 133
bpki_glue
irbe_cli::cmd_elt_mixin, 129
rpki::left_right::child_elt, 317
rpki::left_right::repository_elt, 354
rpki::left_right::self_elt, 364
rpki::publication::client_elt, 420
bpki_https_cert
irbe_cli::cmd_elt_mixin, 129
rpki::left_right::parent_elt, 346
bpki_https_certificate
rpki::myrpki::parent, 402
bpki_https_glue
irbe_cli::cmd_elt_mixin, 129
rpki::left_right::parent_elt, 346
bpki_resources
rpki::myrpki::main, 397
bpki_servers
rpki::myrpki::main, 397
bpki_ta
irdbd, 64
pubd::pubd_context, 169
rootd, 72
rpki::rpki_engine::rpkid_context, 544
bsc
rpki::left_right::data_elt, 322
rpki::myrpki::CA, 375
bscs
rpki::left_right::self_elt, 360
buffer
rpki::https::http_stream, 302
build
rpki::x509::ROA, 649
rpki::x509::SignedManifest, 659
build_https_ta_cache
pubd::pubd_context, 168
rpki::https, 85
rpki::rpki_engine::rpkid_context, 542

ca
rpki::rpki_engine::ca_detail_obj, 507
ca_cert_uri
rpki::rpki_engine::ca_detail_obj, 511
ca_detail
rpki::rpki_engine::child_cert_obj, 522
rpki::rpki_engine::revoked_cert_obj, 530
rpki::rpki_engine::roa_obj, 534
ca_detail_id
rpki::rpki_engine::child_cert_obj, 524
rpki::rpki_engine::revoked_cert_obj, 531
rpki::rpki_engine::roa_obj, 537
ca_details
rpki::rpki_engine::ca_obj, 515
ca_from_class_name
rpki::left_right::child_elt, 315
ca_id
rpki::rpki_engine::ca_detail_obj, 511
cache
rpki::sql::session, 551
cache_clear

rpki::sql::session, 549
calculate_SKI
rpki::x509, 112
call_pubd
irbe_cli, 60
rpki::left_right::repository_elt, 353
rpki::rpki_engine::publication_-queue, 527
call_rpkid
irbe_cli, 60
callback
rpki::https::http_request, 286
caller_function
rpki::async::iterator, 187
cancel
rpki::async::timer, 194
cas
rpki::left_right::parent_elt, 343
cb
rpki::async::sync_wrapper, 190
cer
rpki::myrpki::CA, 378
cert
rpki::https::http_client, 271
rpki::https::http_listener, 275
rpki::https::http_queue, 282
rpki::rpki_engine::child_cert_obj, 524
rpki::rpki_engine::roa_obj, 537
rpki::up_down::certificate_elt, 579
cert_url
rpki::up_down::certificate_elt, 579
rpki::up_down::class_elt, 582
certs
rpki::up_down::class_elt, 582
cfg
irbe_cli, 60
irdbd, 64
rootd, 72
rpki::config::parser, 206
rpki::myrpki::CA, 378
rpki::myrpki::main, 397
cfg_file
irbe_cli, 61
irdbd, 64
pubd, 68
rootd, 72
rpki::myrpki::main, 397
rpkid, 115
characters
rpki::xml_utils::sax_handler, 685
check_allowed_uri
rpki::publication::client_elt, 418
check_for_updates
rpki::rpki_engine::ca_obj, 515
check_response
rpki::up_down::base_elt, 575
rpki::up_down::error_response_pdu, 590
rpki::up_down::issue_response_pdu, 598
check_valid_rpki
rpki::x509::PKCS10, 645
checkpoint
rpki::rpki_engine::rpkid_context, 542
child
rpki::rpki_engine::child_cert_obj, 522
child_bpki_cert
rootd, 72
child_certs
rpki::left_right::child_elt, 315
rpki::rpki_engine::ca_detail_obj, 507
child_id
rpki::rpki_engine::child_cert_obj, 524
children
rpki::left_right::bsc_elt, 310
rpki::left_right::self_elt, 360
chunk_body
rpki::https::http_stream, 297
chunk_discard_crlf
rpki::https::http_stream, 297
chunk_discard_trailer
rpki::https::http_stream, 297
chunk_handler
rpki::https::http_stream, 302
chunk_header
rpki::https::http_stream, 297
class_name

rpki::up_down::class_elt, 582
rpki::up_down::issue_pdu, 595
rpki::up_down::revoke_pdu, 612
rpki::up_down::revoke_syntax, 615
classes
rpki::up_down::class_response_-syntax, 586
clear
rpki::async::timer, 194
rpki::x509::DER_object, 635
clear_https_ta_cache
pubd::pubd_context, 168
rpki::left_right::child_elt, 317
rpki::publication::client_elt, 420
rpki::rpki_engine::rpkid_context, 542
cli.py(3191), 693
client
rpki::https, 85
rpki::https::http_queue, 282
client_cert
rpki::https::caller, 265
client_getopt
irbe_cli::cmd_elt_mixin, 127
client_handler
pubd::pubd_context, 169
client_key
rpki::https::caller, 265
client_poll
rpki::left_right::self_elt, 360
client_query_bpki_cert
irbe_cli::cmd_elt_mixin, 127
client_query_bpki_cms_cert
irbe_cli::cmd_elt_mixin, 127
client_query_bpki_crl
irbe_cli::config_elt, 133
client_query_bpki_https_cert
irbe_cli::cmd_elt_mixin, 128
client_query_cms_glue
irbe_cli::cmd_elt_mixin, 128
client_query_glue
irbe_cli::cmd_elt_mixin, 128
client_query_https_glue
irbe_cli::cmd_elt_mixin, 128
client_query_signing_cert
irbe_cli::bsc_elt, 118
client_query_signing_cert_crl
irbe_cli::bsc_elt, 118
client_queues
rpki::https, 86
client_reply_decode
irbe_cli::bsc_elt, 118
irbe_cli::reply_elt_mixin, 157
client_reply_show
irbe_cli::reply_elt_mixin, 158
client_ta
irdbd, 64
rootd, 72
client_url_regexp
pubd::pubd_context, 169
close
rpki::https::http_stream, 297
rpki::sql::session, 549
cmd
rpki::https::http_request, 286
cmd::Cmd, 115
cmdloop_with_history
rpki::cli::Cmd, 199, 201
cms_msg
irbe_cli::left_right_proto, 139
irbe_cli::publication_proto, 154
cms_xml_sign
rpki::myrpki::CA, 376
cms_xml_verify
rpki::myrpki::CA, 376
code
rpki::https::http_response, 288
codes
rpki::up_down::error_response_pdu, 591
collect_incoming_data
rpki::https::http_stream, 298
columns
rpki::myrpki::csv_reader, 389
rpki::sql::template, 561
comment_characters
rpki::myrpki::csv_reader, 389
complete_help
rpki::cli::Cmd, 199
completedefault
rpki::myrpki::main, 398
completenames

rpki::cli::Cmd, 200
compose_response
rootd, 70
config.py(3107), 693
config_id
rpki::publication::config_elt, 426
configure_resources_main
rpki::myrpki::main, 394
connect
rpki::sql::session, 549
construct_sia_uri
rpki::rpki_engine::ca_obj, 516
contains
rpki::resource_set::resource_set, 470
content
rpki::x509::CMS_object, 622
rpki::x509::DER_CMS_object, 632
rpki::x509::XML_CMS_object, 670
content_class
rpki::x509::ROA, 649
rpki::x509::SignedManifest, 660
control_handler
pubd::pubd_context, 169
convert_to_seconds
rpki::sundial::timedelta, 572
create
rpki::rpki_engine::ca_detail_obj, 507
rpki::rpki_engine::ca_obj, 516
rpki::x509::PKCS10, 645
create_ca
rpki::x509::PKCS10, 645
create_top_level
rpki::xml_utils::sax_handler, 686
crl
rpki::myrpki::CA, 378
crl_interval
rpki::left_right::self_elt, 365
crl_published
rpki::rpki_engine::ca_detail_obj, 511
crl_published_callback
rpki::rpki_engine::ca_detail_obj, 507
crl_uri
rpki::rpki_engine::ca_detail_obj, 507
crl_uri_tail
rpki::rpki_engine::ca_detail_obj, 508
crlnum
rpki::myrpki::CA, 378
cron
rpki::left_right::self_elt, 360
rpki::rpki_engine::rpkid_context, 542
cron_keepalive
rpki::rpki_engine::rpkid_context, 544
cron_period
rpki::rpki_engine::rpkid_context, 544
cron_timeout
rpki::rpki_engine::rpkid_context, 544
cron_timer
rpki::rpki_engine::rpkid_context, 544
cronjob_handler
rpki::rpki_engine::rpkid_context, 542
cross_certify
rpki::x509::X509, 662
csv_writer
rpki::myrpki, 96
cur
irdbd, 64
rpki::sql::session, 551

database
rpki::sql::session, 551
datum_type
rpki::resource_set::resource_range_-as, 459
rpki::resource_set::resource_range_-ipv4, 465
rpki::resource_set::resource_range_-ipv6, 467
db
irdbd, 64
rpki::sql::session, 551

debug
rpki::https::caller, 266
rpki::log, 92
debug_cms_certs
rpki::x509::CMS_object, 622
debug_http
rpki::https, 86
debug_tls_certs
rpki::https, 86
decode
rpki::x509::DER_CMS_object, 632
rpki::x509::XML_CMS_object, 668
default_client_timeout
rpki::https, 86
default_http_version
rpki::https, 86
default_pubd_handler
rpki::left_right::repository_elt, 353
default_section
rpki::config::parser, 207
default_server_timeout
rpki::https, 86
defer
rpki::async, 77
deferred_queue
rpki::async, 78
del_subject_cert
rootd, 70
del_subject_pkcs10
rootd, 70
delete
rpki::rpki_engine::ca_detail_obj, 508
rpki::rpki_engine::ca_obj, 516
rpki::sql::template, 561
DER
rpki::x509::CMS_object, 623
rpki::x509::CRL, 628
rpki::x509::DER_object, 640
rpki::x509::PKCS10, 646
rpki::x509::RSA, 653
rpki::x509::RSApublic, 657
rpki::x509::X509, 665
description
rpki::up_down::error_response_pdu, 591
detach
rpki::https::http_queue, 281
dict, 115
difference
rpki::resource_set::resource_set, 470
dir
rpki::myrpki::CA, 378
rpki::myrpki::EntityDB, 392
dirty
rpki::sql::session, 551
do_configure_child
rpki::myrpki::main, 395
do_configure_daemons
rpki::myrpki::main, 395
do_configure_parent
rpki::myrpki::main, 395
do_configure_publication_client
rpki::myrpki::main, 396
do_configure_repository
rpki::myrpki::main, 396
do_configure_resources
rpki::myrpki::main, 396
do_EOF
rpki::cli::Cmd, 200
do_exit
rpki::cli::Cmd, 200
do_initialize
rpki::myrpki::main, 396
do_quit
rpki::cli::Cmd, 201
doit
rpki::async::iterator, 187
done_callback
rpki::async::iterator, 187
dump
rpki::x509::DeadDrop, 630
dump_inbound_cms
rpki::x509::XML_CMS_object, 670
dump_on_verify_failure
rpki::x509::CMS_object, 623
dump_outbound_cms
rpki::x509::XML_CMS_object, 670
dump_to_disk
rpki::x509::XML_CMS_object, 668
dumpasn1
rpki::x509::DER_object, 635

dynamic_ta
rpki::https::http_listener, 275

e
rpki::x509::PEM_converter, 643
earlier
rpki::sundial::datetime, 565
eb
rpki::async::sync_wrapper, 190
econtent_oid
rpki::x509::CMS_object, 623
rpki::x509::ROA, 649
rpki::x509::SignedManifest, 660
rpki::x509::XML_CMS_object, 670
ee
rpki::myrpki::CA, 376
element_name
rpki::left_right::bsc_elt, 312
rpki::left_right::child_elt, 317
rpki::left_right::list_published_-objects_elt, 329
rpki::left_right::list_received_-resources_elt, 331
rpki::left_right::list_resources_elt, 335
rpki::left_right::list_roa_requests_-elt, 337
rpki::left_right::parent_elt, 346
rpki::left_right::report_error_elt, 350
rpki::left_right::repository_elt, 354
rpki::left_right::self_elt, 365
rpki::publication::certificate_elt, 416
rpki::publication::client_elt, 420
rpki::publication::config_elt, 427
rpki::publication::crl_elt, 432
rpki::publication::manifest_elt, 434
rpki::publication::report_error_elt, 446
rpki::publication::roa_elt, 449
elements
rpki::left_right::bsc_elt, 312
rpki::left_right::child_elt, 318
rpki::left_right::parent_elt, 346
rpki::left_right::repository_elt, 355
rpki::left_right::self_elt, 365
rpki::publication::client_elt, 420
rpki::publication::config_elt, 427
rpki::xml_utils::base_elt, 674
empty
rpki::resource_set::resource_bag, 454
rpki::x509::DER_object, 635
emptyline
rpki::cli::Cmd, 200
emptyline_repeats_last_command
rpki::cli::Cmd, 201
enable_trace
rpki::log, 92
encode
rpki::x509::DER_CMS_object, 632
rpki::x509::XML_CMS_object, 668
encoding
rpki::left_right::cms_msg, 320
rpki::publication::cms_msg, 423
rpki::up_down::cms_msg, 588
endElement
rpki::left_right::child_elt, 316
rpki::publication::client_elt, 418
rpki::publication::publication_-object_elt, 440
rpki::up_down::base_elt, 575
rpki::up_down::certificate_elt, 578
rpki::up_down::class_elt, 581
rpki::up_down::error_response_pdu, 590
rpki::up_down::issue_pdu, 594
rpki::xml_utils::base_elt, 672
rpki::xml_utils::data_elt, 677
rpki::xml_utils::msg, 682
rpki::xml_utils::sax_handler, 686
rpki::xml_utils::text_elt, 689
endElementNS
rpki::xml_utils::sax_handler, 686
enforce_strict_up_down_xml_sender
rpki::left_right, 90
entitydb
rpki::myrpki::main, 398
env
rpki::myrpki::CA, 379
EOF_exits_command_loop
rpki::cli::Cmd, 202
err

rpki::async::sync_wrapper, 191
errback
rpki::async::timer, 194, 196
rpki::https::http_request, 286
error
rpki::log, 92
error_code
rpki::left_right::report_error_elt, 350
rpki::publication::report_error_elt, 446
error_text
rpki::left_right::report_error_elt, 350
rpki::publication::report_error_elt, 446
etree_post_read
rpki::myrpki, 96
etree_pre_write
rpki::myrpki, 96
etree_read
rpki::myrpki, 97
etree_validate
rpki::myrpki, 97
etree_write
rpki::myrpki, 97
event_loop
rpki::async, 78
Exception, 116
exceptions
rpki::up_down::error_response_pdu, 591
exceptions.py(2907), 693
excludes
irbe_cli::bsc_elt, 119
irbe_cli::cmd_elt_mixin, 129
irbe_cli::list_published_objects_elt, 143
irbe_cli::list_received_resources_elt, 145
execute
rpki::sql::session, 549
executemany
rpki::sql::session, 550
exit_event_loop
rpki::async, 78
ExitNow
rpki::async, 78
expect_close
rpki::https::http_client, 271
rpki::https::http_server, 293
expired
rpki::x509::X509, 663
expires
rpki::rpki_engine::revoked_cert_obj, 531
explicitVersion
rpki::manifest::Manifest, 372
rpki::roa::RouteOriginAttestation, 503
extract
rpki::x509::CMS_object, 621

fetch
rpki::publication::config_elt, 425
rpki::rpki_engine::child_cert_obj, 523
fetch_active
rpki::rpki_engine::ca_obj, 516
fetch_deprecated
rpki::rpki_engine::ca_obj, 517
fetch_issue_response_candidates
rpki::rpki_engine::ca_obj, 517
fetch_pending
rpki::rpki_engine::ca_obj, 517
fetch_revoked
rpki::rpki_engine::ca_obj, 517
fetchall
rpki::sql::session, 550
file
rpki::manifest::FileAndHash, 369
rpki::myrpki::csv_reader, 389
fileHashAlg
rpki::manifest::Manifest, 372
fileList
rpki::manifest::Manifest, 372
filename
rpki::config::parser, 207
rpki::myrpki::csv_reader, 390
filename_complete
rpki::cli::Cmd, 200
find_handler
rpki::https::http_server, 291
format

rpki::https::http_message, 277
format_first_line
rpki::https::http_request, 285
rpki::https::http_response, 288
formats
rpki::x509::CMS_object, 623
rpki::x509::CRL, 628
rpki::x509::DER_object, 640
rpki::x509::PKCS10, 646
rpki::x509::RSA, 653
rpki::x509::RSApublic, 657
rpki::x509::X509, 665
found_terminator
rpki::https::http_stream, 298
from_bytes
rpki::ipaddrs::v4addr, 304
rpki::ipaddrs::v6addr, 307
from_csv
rpki::myrpki::children, 386
rpki::myrpki::parents, 404
rpki::myrpki::repositories, 406
rpki::myrpki::roa_requests, 414
from_exception
rpki::left_right::report_error_elt, 349
rpki::publication::report_error_elt, 445
from_resource_bag
rpki::up_down::class_elt, 581
from_rfc3779_tuples
rpki::resource_set::resource_bag, 454
from_sql
rpki::resource_set::resource_set, 470
rpki::resource_set::roa_prefix_set, 491
rpki::sundial::datetime, 565
rpki::x509::DER_object, 636
fromASN1tuple
rpki::sundial::datetime, 565
fromdatetime
rpki::sundial::datetime, 565
fromGeneralizedTime
rpki::sundial::datetime, 566
fromtimedelta
rpki::sundial::timedelta, 572
fromUTCTime
rpki::sundial::datetime, 566
fromXMLtime
rpki::sundial::datetime, 566
func
rpki::async::sync_wrapper, 191
fxcert
rpki::myrpki::CA, 376

gAKI
rpki::x509::DER_object, 636
gc_debug
rpki::async::timer, 196
gctx
rpki::rpki_engine::ca_detail_obj, 511
rpki::rpki_engine::ca_obj, 519
rpki::rpki_engine::child_cert_obj, 524
rpki::rpki_engine::revoked_cert_obj, 531
rpki::rpki_engine::roa_obj, 538
rpki::sql::sql_persistent, 558
generate
rpki::rpki_engine::roa_obj, 535
rpki::x509::CRL, 626
rpki::x509::RSA, 652
generate_crl
rpki::rpki_engine::ca_detail_obj, 508
generate_manifest
rpki::rpki_engine::ca_detail_obj, 508
generate_manifest_cert
rpki::rpki_engine::ca_detail_obj, 508
get
rpki::config::parser, 205
get_3779resources
rpki::x509::DER_object, 636
get_AIA
rpki::x509::DER_object, 636
get_aia_uri
rpki::x509::DER_object, 636
get_AKI
rpki::x509::DER_object, 637
get_Base64

rpki::x509::DER_object, 637
get_basicConstraints
rpki::x509::DER_object, 637
get_buffer
rpki::https::http_stream, 298
get_content
rpki::x509::CMS_object, 621
get_DER
rpki::x509::CMS_object, 621
rpki::x509::CRL, 626
rpki::x509::DER_object, 637
rpki::x509::PKCS10, 646
rpki::x509::RSA, 652
rpki::x509::RSApublic, 656
rpki::x509::X509, 663
get_PEM
rpki::x509::DER_object, 637
get_POW
rpki::x509::CMS_object, 621
rpki::x509::CRL, 627
rpki::x509::RSA, 652
rpki::x509::RSApublic, 656
rpki::x509::X509, 663
get_POWpkix
rpki::x509::CRL, 627
rpki::x509::PKCS10, 646
rpki::x509::X509, 663
get_public_DER
rpki::x509::RSA, 653
get_root_cert
rootd, 70
get_RSApublic
rpki::x509::RSA, 653
get_SIA
rpki::x509::DER_object, 638
get_sia_directory_uri
rpki::x509::DER_object, 638
get_sia_manifest_uri
rpki::x509::DER_object, 638
get_SKI
rpki::up_down::revoke_pdu, 611
rpki::x509::DER_object, 638
rpki::x509::RSA, 653
rpki::x509::RSApublic, 656
get_subject_cert
rootd, 71
get_subject_pkcs10
rootd, 71
getboolean
rpki::config::parser, 205
getint
rpki::config::parser, 205
getIssuer
rpki::x509::CRL, 627
rpki::x509::X509, 663
getlong
rpki::config::parser, 205
getNextUpdate
rpki::x509::CRL, 627
rpki::x509::SignedManifest, 659
getNotAfter
rpki::x509::X509, 663
getNotBefore
rpki::x509::X509, 664
getPublicKey
rpki::x509::PKCS10, 646
rpki::x509::X509, 664
getSerial
rpki::x509::X509, 664
getSubject
rpki::x509::X509, 664
getThisUpdate
rpki::x509::CRL, 627
rpki::x509::SignedManifest, 659
group
rpki::myrpki::roa_request, 412
gSKI
rpki::x509::DER_object, 638

hAKI
rpki::x509::DER_object, 639
handle
rpki::myrpki::child, 383
rpki::myrpki::main, 398
rpki::myrpki::parent, 402
rpki::myrpki::repository, 408
handle_accept
rpki::https::http_listener, 274
handle_body
rpki::https::http_stream, 298
handle_close
rpki::https::http_client, 268

rpki::https::http_stream, 299
handle_connect
rpki::https::http_client, 269
handle_dispatch
irdbd, 65
handle_error
rpki::https::http_client, 269
rpki::https::http_listener, 274
rpki::https::http_stream, 299
handle_list_resources
irdbd, 63
handle_list_roa_requests
irdbd, 63
handle_message
rpki::https::http_client, 269
rpki::https::http_server, 291
handle_no_content_length
rpki::https::http_client, 269
rpki::https::http_server, 292
handle_read
rpki::https::http_stream, 299
handle_timeout
rpki::https::http_client, 270
rpki::https::http_stream, 299
handle_write
rpki::https::http_stream, 300
handler
irdbd, 64
rpki::async::gc_summary, 184
rpki::async::timer, 195, 197
handler_common
pubd::pubd_context, 169
handlers
irdbd, 65
rootd, 72
rpki::https::http_listener, 275
rpki::https::http_server, 293
rpki::rpki_engine::publication_-queue, 528
handles
rpki::left_right::bsc_elt, 312
rpki::left_right::child_elt, 318
rpki::left_right::data_elt, 324
rpki::left_right::parent_elt, 346
rpki::left_right::repository_elt, 355
rpki::left_right::self_elt, 365
has_option
rpki::config::parser, 205
has_section
rpki::config::parser, 206
hash
rpki::manifest::FileAndHash, 369
have_readline
rpki::cli, 80
headers
rpki::https::http_message, 279
help_help
rpki::cli::Cmd, 201
help_overview
rpki::myrpki::main, 397
histfile
rpki::cli::Cmd, 202
rpki::myrpki::main, 398
host
irdbd, 65
rootd, 72
hostport
rpki::https::http_client, 271
rpki::https::http_queue, 283
hSKI
rpki::x509::DER_object, 639
https.py(3191), 695
https_server_host
pubd::pubd_context, 170
rootd, 73
rpki::rpki_engine::rpkid_context, 545
https_server_port
pubd::pubd_context, 170
rootd, 73
rpki::rpki_engine::rpkid_context, 545
https_ta_cache
pubd::pubd_context, 170
rpki::rpki_engine::rpkid_context, 545

identchars
rpki::cli::Cmd, 202
index
rpki::myrpki::CA, 379
rpki::sql::template, 561

info
rpki::log, 92
inherit
rpki::resource_set::resource_set, 471
rpki::resource_set::resource_set_as, 474
rpki::resource_set::resource_set_ip, 477
inherit_token
rpki::resource_set, 104
init
rpki::log, 91
initial_delay
rpki::rpki_engine::rpkid_context, 545
initiate_send
rpki::https::http_stream, 300
insert
rpki::sql::template, 561
intersection
rpki::resource_set::resource_bag, 454
rpki::resource_set::resource_set, 470
interval
rpki::async::gc_summary, 184
ipAddrBlocks
rpki::roa::RouteOriginAttestation, 503
ipaddrs.py(2424), 696
ipv4
rpki::left_right::list_resources_elt, 335
rpki::left_right::list_roa_requests_-elt, 338
rpki::rpki_engine::roa_obj, 538
ipv6
rpki::left_right::list_resources_elt, 335
rpki::left_right::list_roa_requests_-elt, 338
rpki::rpki_engine::roa_obj, 538
irbe_cert
pubd::pubd_context, 170
rpki::rpki_engine::rpkid_context, 545
irbe_cli, 58
argv, 60
call_pubd, 60
call_rpkid, 60
cfg, 60
cfg_file, 61
pem_out, 61
q_msg, 61
q_msg_left_right, 61
q_msg_publication, 61
q_pdu, 61
top_opts, 61
usage, 60
usage_fill, 62
verbose, 62
irbe_cli.py(3107), 697
irbe_cli::bsc_elt, 116
client_query_signing_cert, 118
client_query_signing_cert_crl, 118
client_reply_decode, 118
excludes, 119
signing_cert, 119
signing_cert_crl, 119
irbe_cli::certificate_elt, 119
irbe_cli::child_elt, 121
irbe_cli::client_elt, 123
irbe_cli::cmd_elt_mixin, 125
bpki_cert, 129
bpki_cms_cert, 129
bpki_cms_glue, 129
bpki_glue, 129
bpki_https_cert, 129
bpki_https_glue, 129
client_getopt, 127
client_query_bpki_cert, 127
client_query_bpki_cms_cert, 127
client_query_bpki_https_cert, 128
client_query_cms_glue, 128
client_query_glue, 128
client_query_https_glue, 128
excludes, 129
is_cmd, 130
usage, 128
irbe_cli::cmd_msg_mixin, 130
usage, 131
irbe_cli::config_elt, 131
bpki_crl, 133

client_query_bpki_crl, 133
irbe_cli::crl_elt, 133
irbe_cli::left_right_cms_msg, 135
saxify, 136
irbe_cli::left_right_msg, 136
pdus, 138
irbe_cli::left_right_proto, 138
cms_msg, 139
msg, 139
irbe_cli::left_right_sax_handler, 140
pdu, 141
irbe_cli::list_published_objects_elt, 141
excludes, 143
irbe_cli::list_received_resources_elt, 143
excludes, 145
irbe_cli::manifest_elt, 145
irbe_cli::parent_elt, 147
irbe_cli::publication_cms_msg, 149
saxify, 151
irbe_cli::publication_msg, 151
pdus, 153
irbe_cli::publication_proto, 153
cms_msg, 154
msg, 154
irbe_cli::publication_sax_handler, 155
pdu, 156
irbe_cli::reply_elt_mixin, 156
client_reply_decode, 157
client_reply_show, 158
is_cmd, 158
irbe_cli::report_error_elt, 158
irbe_cli::repository_elt, 159
irbe_cli::roa_elt, 161
irbe_cli::self_elt, 163
irbe_cli::UsageWrapper, 165
__call__, 166
irdb_cert
rpki::rpki_engine::rpkid_context, 545
irdb_query
rpki::rpki_engine::rpkid_context, 543
irdb_query_child_resources
rpki::rpki_engine::rpkid_context, 543
irdb_query_roa_requests
rpki::rpki_engine::rpkid_context, 543
irdb_url
rpki::rpki_engine::rpkid_context, 545
irdbd, 62
bpki_ta, 64
cfg, 64
cfg_file, 64
client_ta, 64
cur, 64
db, 64
handle_dispatch, 65
handle_list_resources, 63
handle_list_roa_requests, 63
handler, 64
handlers, 65
host, 65
irdbd_cert, 65
irdbd_key, 65
port, 65
rpkid_cert, 66
server_cert, 66
startup_msg, 66
u, 66
irdbd.py(2913), 698
irdbd_cert
irdbd, 65
irdbd_key
irdbd, 65
is_CA
rpki::x509::DER_object, 639
is_cmd
irbe_cli::cmd_elt_mixin, 130
irbe_cli::reply_elt_mixin, 158
is_query
rpki::xml_utils::msg, 682
is_reply
rpki::xml_utils::msg, 682
is_set
rpki::async::timer, 195
issubset
rpki::resource_set::resource_set, 470
issue
rpki::rpki_engine::ca_detail_obj, 509

rpki::x509::X509, 664
issue_ee
rpki::rpki_engine::ca_detail_obj, 509
issue_subject_cert_maybe
rootd, 71
issuer
rpki::up_down::class_elt, 583
issuperset
rpki::resource_set::resource_set, 471
item_callback
rpki::async::iterator, 187
iterate
rpki::myrpki::EntityDB, 392
iterator
rpki::async::iterator, 187

key
rpki::https::http_client, 271
rpki::https::http_listener, 275
rpki::https::http_queue, 283
rpki::myrpki::CA, 379

last_crl_sn
rpki::rpki_engine::ca_obj, 519
last_issued_sn
rpki::rpki_engine::ca_obj, 519
last_manifest_sn
rpki::rpki_engine::ca_obj, 519
lastrowid
rpki::sql::session, 550
later
rpki::sundial::datetime, 566
latest_ca_cert
rpki::rpki_engine::ca_detail_obj, 511
latest_crl
rpki::rpki_engine::ca_detail_obj, 511
latest_manifest
rpki::rpki_engine::ca_detail_obj, 512
latest_manifest_cert
rpki::rpki_engine::ca_detail_obj, 512
left_right
rpki::relaxng, 101
left_right.py(3191), 699
left_right_handler
rpki::rpki_engine::rpkid_context, 543
log
rpki::https::http_listener, 275
rpki::https::http_queue, 283
rpki::https::http_stream, 302
log.py(3107), 699
log_cert
rpki::https::http_stream, 300
log_method
rpki::https, 85
log_query
rootd::message_pdu, 179
rpki::up_down::message_pdu, 604
long, 166
looks_like_PEM
rpki::x509::PEM_converter, 642

maildir
rpki::x509::DeadDrop, 630
main
pubd, 67
rpkid, 114
make_b64elt
rpki::up_down::base_elt, 575
rpki::xml_utils::base_elt, 673
make_elt
rpki::up_down::base_elt, 575
rpki::xml_utils::base_elt, 673
make_pdu
rpki::xml_utils::base_elt, 673
make_prefix
rpki::resource_set::resource_range_-ip, 462
make_publish
rpki::publication::publication_-object_elt, 440
make_query
rpki::up_down::message_pdu, 604
make_reply
rpki::left_right::list_published_-objects_elt, 328

rpki::left_right::list_received_-resources_elt, 331
rpki::xml_utils::data_elt, 677
make_reply_clone_hook
rpki::left_right::data_elt, 322
rpki::xml_utils::data_elt, 677
make_withdraw
rpki::publication::publication_-object_elt, 441
manifest.py(2424), 700
manifest_private_key_id
rpki::rpki_engine::ca_detail_obj, 512
manifest_public_key
rpki::rpki_engine::ca_detail_obj, 512
manifest_published
rpki::rpki_engine::ca_detail_obj, 512
manifest_published_callback
rpki::rpki_engine::ca_detail_obj, 509
manifest_uri
rpki::rpki_engine::ca_detail_obj, 509
manifestNumber
rpki::manifest::Manifest, 372
map
rpki::sql::template, 562
max
rpki::resource_set::resource_range, 457
rpki::resource_set::roa_prefix, 483
max_prefixlen
rpki::resource_set::roa_prefix, 484
maxLength
rpki::roa::ROAIPAddress, 498
min
rpki::resource_set::resource_range, 457
rpki::resource_set::resource_range_-as, 460
rpki::resource_set::roa_prefix, 484
min_columns
rpki::myrpki::csv_reader, 390
msg
irbe_cli::left_right_proto, 139
irbe_cli::publication_proto, 154
rpki::https::http_stream, 302
msgs
rpki::rpki_engine::publication_-queue, 528
multiget
rpki::config::parser, 206
myhandle
rpki::myrpki::parent, 402
myrpki.py, 700

name
rpki::left_right::sax_handler, 357
rpki::publication::sax_handler, 451
rpki::up_down::sax_handler, 618
name2oid
rpki::oids, 99
name2type
rootd::message_pdu, 179
rpki::up_down::message_pdu, 606
namespace
rpki::myrpki, 98
namespaceQName
rpki::myrpki, 98
next_crl_number
rpki::rpki_engine::ca_obj, 517
next_manifest_number
rpki::rpki_engine::ca_obj, 518
next_serial_number
rpki::rpki_engine::ca_obj, 518
nextUpdate
rpki::manifest::Manifest, 372
rpki::rpki_engine::ca_detail_obj, 512
normalize_chain
rpki::x509::X509, 665
normalize_headers
rpki::https::http_message, 278
note
rpki::log, 93
now
rpki::sundial, 108
nsmap
rpki::left_right::left_right_-namespace, 325

rpki::publication::publication_-namespace, 438
rpki::up_down, 110

obj
rpki::left_right::list_published_-objects_elt, 329
object, 166
oid2name
rpki::oids, 99
oids.py(2424), 701
onecmd
rpki::cli::Cmd, 201
openssl
rpki::myrpki::CA, 379
other_clear
rpki::x509::CMS_object, 623
rpki::x509::DER_object, 640
oversized
rpki::resource_set::resource_bag, 454

parent
rpki::rpki_engine::ca_obj, 518
parent_id
rpki::rpki_engine::ca_obj, 519
parent_resource_class
rpki::rpki_engine::ca_obj, 519
parents
rpki::left_right::bsc_elt, 310
rpki::left_right::child_elt, 316
rpki::left_right::repository_elt, 354
rpki::left_right::self_elt, 360
parse
rpki::sundial::timedelta, 573
parse_first_line
rpki::https::http_request, 285
rpki::https::http_response, 288
parse_from_wire
rpki::https::http_message, 278
parse_rfc3779_tuple
rpki::resource_set::resource_set_as, 473
rpki::resource_set::resource_set_ip, 476
parse_str
rpki::resource_set::resource_set_as, 473
rpki::resource_set::resource_set_ip, 476
rpki::resource_set::roa_prefix_set, 491
parse_type
rpki::https::http_client, 271
rpki::https::http_server, 293
parse_version
rpki::https::http_message, 278
password
rpki::sql::session, 551
path
rpki::https::http_request, 286
path_restriction
rpki::myrpki::CA, 379
payload
rpki::publication::publication_-object_elt, 442
rpki::up_down::message_pdu, 606
payload_type
rpki::publication::certificate_elt, 416
rpki::publication::crl_elt, 432
rpki::publication::manifest_elt, 434
rpki::publication::publication_-object_elt, 442
rpki::publication::roa_elt, 449
pdu
irbe_cli::left_right_sax_handler, 141
irbe_cli::publication_sax_handler, 156
rootd::sax_handler, 183
rpki::left_right::sax_handler, 357
rpki::publication::sax_handler, 451
rpki::up_down::sax_handler, 618
pdus
irbe_cli::left_right_msg, 138
irbe_cli::publication_msg, 153
rpki::left_right::msg, 340
rpki::publication::msg, 436
pem_converter
rpki::x509::CMS_object, 624
rpki::x509::CRL, 628
rpki::x509::DER_object, 640
rpki::x509::PKCS10, 647

rpki::x509::ROA, 649
rpki::x509::RSA, 654
rpki::x509::RSApublic, 657
rpki::x509::SignedManifest, 660
rpki::x509::X509, 665
pem_out
irbe_cli, 61
PEMElement
rpki::myrpki, 97
persistent
rpki::https::http_message, 278
pid
rpki::log, 93
rpki::x509::DeadDrop, 630
ping
rpki::sql::session, 550
pkcs10
rpki::up_down::issue_pdu, 595
pkcs10_request
rpki::left_right::bsc_elt, 312
PKIX_threshhold
rpki::sundial::datetime, 568
port
irdbd, 65
rootd, 73
POW
rpki::x509::CMS_object, 624
rpki::x509::CRL, 628
rpki::x509::RSA, 654
rpki::x509::RSApublic, 657
rpki::x509::X509, 666
POWify_OID
rpki::x509, 112
POWpkix
rpki::x509::CRL, 628
rpki::x509::PKCS10, 647
rpki::x509::X509, 666
prefix
rpki::resource_set::roa_prefix, 484
prefix_type
rpki::resource_set::roa_prefix_set_-ipv4, 494
rpki::resource_set::roa_prefix_set_-ipv6, 496
prefixlen
rpki::resource_set::roa_prefix, 485
pretty_print_content
rpki::x509::XML_CMS_object, 669
print_on_der_error
rpki::x509::CMS_object, 624
priority
rpki::log::logger, 367
private_key_id
rpki::left_right::bsc_elt, 312
rpki::rpki_engine::ca_detail_obj, 512
profile
pubd, 68
rpkid, 115
prompt
rpki::myrpki::main, 398
proto
rpki::https::caller, 266
pubd, 66
cfg_file, 68
main, 67
profile, 68
pubd.py(3107), 702
pubd::pubd_context, 166
__init__, 168
bpki_ta, 169
build_https_ta_cache, 168
clear_https_ta_cache, 168
client_handler, 169
client_url_regexp, 169
control_handler, 169
handler_common, 169
https_server_host, 170
https_server_port, 170
https_ta_cache, 170
irbe_cert, 170
pubd_cert, 170
pubd_key, 170
publication_base, 170
publication_multimodule, 171
sql, 171
pubd_cert
pubd::pubd_context, 170
pubd_contact_info
rpki::myrpki::main, 398
pubd_key
pubd::pubd_context, 170

public_key
rpki::rpki_engine::ca_detail_obj, 513
publication
rpki::relaxng, 101
publication.py(3107), 702
publication_base
pubd::pubd_context, 170
publication_kludge_base
rpki::rpki_engine::rpkid_context, 546
publication_multimodule
pubd::pubd_context, 171
publish
rpki::rpki_engine::publication_-queue, 527
published
rpki::rpki_engine::child_cert_obj, 524
rpki::rpki_engine::roa_obj, 538
published_callback
rpki::rpki_engine::child_cert_obj, 523
rpki::rpki_engine::roa_obj, 535
pydatetime::datetime, 171
pydatetime::timedelta, 171

q_msg
irbe_cli, 61
q_msg_left_right
irbe_cli, 61
q_msg_publication
irbe_cli, 61
q_pdu
irbe_cli, 61
query
rpki::up_down::issue_pdu, 594
rpki::up_down::list_pdu, 600
rpki::up_down::revoke_pdu, 611
rpki::xml_utils::msg, 682
query_up_down
rpki::left_right::parent_elt, 343
queue
rpki::async::timer, 197
rpki::https::http_client, 272
rpki::https::http_queue, 283

raise_if_error
rpki::publication::publication_-object_elt, 441
rpki::publication::report_error_elt, 446
range_type
rpki::resource_set::resource_set_as, 474
rpki::resource_set::resource_set_-ipv4, 479
rpki::resource_set::resource_set_-ipv6, 481
rpki::resource_set::roa_prefix_ipv4, 487
rpki::resource_set::roa_prefix_ipv6, 489
read_attrs
rpki::xml_utils::base_elt, 673
read_config
rpki::myrpki::main, 397
readable
rpki::https::http_stream, 300
reason
rpki::https::http_response, 288
recipient
rpki::up_down::message_pdu, 606
recv
rpki::https::http_stream, 300
regen_margin
rpki::left_right::self_elt, 365
regenerate
rpki::rpki_engine::roa_obj, 535
regenerate_crls_and_manifests
rpki::left_right::self_elt, 361
regexp
rpki::sundial::timedelta, 573
reissue
rpki::rpki_engine::child_cert_obj, 523
rekey
rpki::rpki_engine::ca_obj, 518
relaxng.py(3110), 703
replace
rpki::rpki_engine::publication_-queue, 528
reply

rpki::xml_utils::msg, 683
repositories
rpki::left_right::bsc_elt, 311
rpki::left_right::self_elt, 361
rpki::rpki_engine::publication_-queue, 528
repository
rpki::left_right::parent_elt, 344
req
rpki::myrpki::CA, 379
req_resource_set_as
rpki::up_down::certificate_elt, 579
rpki::up_down::issue_pdu, 595
req_resource_set_ipv4
rpki::up_down::certificate_elt, 579
rpki::up_down::issue_pdu, 595
req_resource_set_ipv6
rpki::up_down::certificate_elt, 579
rpki::up_down::issue_pdu, 595
request
rpki::https::http_queue, 281
require_crls
rpki::x509::CMS_object, 624
res
rpki::async::sync_wrapper, 191
resource_set.py(3107), 703
resource_set_as
rpki::up_down::class_elt, 583
resource_set_ipv4
rpki::up_down::class_elt, 583
resource_set_ipv6
rpki::up_down::class_elt, 583
resource_set_notafter
rpki::up_down::class_elt, 583
resource_set_type
rpki::resource_set::roa_prefix_set_-ipv4, 494
rpki::resource_set::roa_prefix_set_-ipv6, 496
restart
rpki::https::http_queue, 282
rpki::https::http_stream, 301
result
rpki::xml_utils::sax_handler, 687
retried
rpki::https::http_request, 286
retry_read
rpki::https::http_client, 272
rpki::https::http_server, 293
rpki::https::http_stream, 302
retry_write
rpki::https::http_client, 272
rpki::https::http_server, 293
rpki::https::http_stream, 302
return_result
rpki::https::http_queue, 282
revoke
rpki::rpki_engine::ca_detail_obj, 509
rpki::rpki_engine::ca_obj, 518
rpki::rpki_engine::child_cert_obj, 523
rpki::rpki_engine::revoked_cert_obj, 530
rpki::rpki_engine::roa_obj, 535
revoked
rpki::rpki_engine::revoked_cert_obj, 531
revoked_certs
rpki::rpki_engine::ca_detail_obj, 510
roa
rpki::rpki_engine::roa_obj, 538
roa.py(2424), 704
roas
rpki::left_right::self_elt, 361
rpki::rpki_engine::ca_detail_obj, 510
root_newer_than_subject
rootd, 71
rootd, 68
bpki_ta, 72
cfg, 72
cfg_file, 72
child_bpki_cert, 72
client_ta, 72
compose_response, 70
del_subject_cert, 70
del_subject_pkcs10, 70
get_root_cert, 70
get_subject_cert, 71
get_subject_pkcs10, 71

handlers, 72
host, 72
https_server_host, 73
https_server_port, 73
issue_subject_cert_maybe, 71
port, 73
root_newer_than_subject, 71
rootd_bpki_cert, 73
rootd_bpki_crl, 73
rootd_bpki_key, 73
rpki_base_uri, 73
rpki_class_name, 74
rpki_root_cert, 74
rpki_root_cert_file, 74
rpki_root_cert_uri, 74
rpki_root_crl, 74
rpki_root_dir, 74
rpki_root_key, 74
rpki_root_manifest, 75
rpki_subject_cert, 75
rpki_subject_lifetime, 75
rpki_subject_pkcs10, 75
rpki_subject_regen, 75
server_cert, 75
set_subject_cert, 71
set_subject_pkcs10, 71
up_down_handler, 71
rootd.py(2913), 705
rootd::cms_msg, 171
saxify, 173
rootd::issue_pdu, 173
serve_pdu, 175
rootd::list_pdu, 175
serve_pdu, 177
rootd::message_pdu, 177
log_query, 179
name2type, 179
type2name, 179
rootd::revoke_pdu, 180
serve_pdu, 181
rootd::sax_handler, 181
pdu, 183
rootd_bpki_cert
rootd, 73
rootd_bpki_crl
rootd, 73
rootd_bpki_key
rootd, 73
rpki, 76
rpki.__doc__, 76
rpki.async, 76
rpki.cli, 79
rpki.config, 80
rpki.exceptions, 81
rpki.https, 83
rpki.ipaddrs, 88
rpki.left_right, 89
rpki.log, 90
rpki.manifest, 93
rpki.myrpki, 94
rpki.oids, 98
rpki.publication, 100
rpki.relaxng, 101
rpki.resource_set, 102
rpki.roa, 104
rpki.rpki_engine, 106
rpki.sql, 106
rpki.sundial, 107
rpki.up_down, 109
rpki.x509, 111
rpki.xml_utils, 113
rpki::async
_raiseExitNow, 77
defer, 77
deferred_queue, 78
event_loop, 78
exit_event_loop, 78
ExitNow, 78
run_deferred, 78
rpki::async::gc_summary, 183
__init__, 184
handler, 184
interval, 184
threshold, 184
timer, 184
rpki::async::iterator, 185
__call__, 186
__init__, 186
__repr__, 187
caller_function, 187
doit, 187
done_callback, 187

item_callback, 187
iterator, 187
unwind_stack, 188
rpki::async::sync_wrapper, 188
__call__, 190
__init__, 190
cb, 190
eb, 190
err, 191
func, 191
res, 191
rpki::async::timer, 191
__cmp__, 194
__del__, 194
__init__, 194
__repr__, 194
cancel, 194
clear, 194
errback, 194, 196
gc_debug, 196
handler, 195, 197
is_set, 195
queue, 197
run_debug, 197
runq, 195
seconds_until_wakeup, 195
set, 195
set_errback, 196
set_handler, 196
trace, 196
when, 197
rpki::cli
_yes_or_no_prompts, 80
have_readline, 80
yes_or_no, 79
rpki::cli::Cmd, 197
__init__, 199
cmdloop_with_history, 199, 201
complete_help, 199
completenames, 200
do_EOF, 200
do_exit, 200
do_quit, 201
emptyline, 200
emptyline_repeats_last_command, 201
EOF_exits_command_loop, 202
filename_complete, 200
help_help, 201
histfile, 202
identchars, 202
onecmd, 201
rpki::config::parser, 202
__init__, 204
_regexp, 206
_repl, 204
cfg, 206
default_section, 207
filename, 207
get, 205
getboolean, 205
getint, 205
getlong, 205
has_option, 205
has_section, 206
multiget, 206
set_global_flags, 206
rpki::exceptions::BadClassNameSyntax, 207
rpki::exceptions::BadClientURL, 208
rpki::exceptions::BadContactURL, 209
rpki::exceptions::BadExtension, 210
rpki::exceptions::BadIRDBReply, 211
rpki::exceptions::BadIssueResponse, 212
rpki::exceptions::BadPKCS10, 213
rpki::exceptions::BadPublicationReply, 214
rpki::exceptions::BadQuery, 215
rpki::exceptions::BadSender, 216
rpki::exceptions::BadStatusCode, 217
rpki::exceptions::BadURISyntax, 218
rpki::exceptions::BSCNotFound, 219
rpki::exceptions::BSCNotReady, 220
rpki::exceptions::ChildNotFound, 221
rpki::exceptions::ClassNameMismatch, 222
rpki::exceptions::ClassNameUnknown, 223
rpki::exceptions::ClientNotFound, 224
rpki::exceptions::CMSContentNotSet, 225
rpki::exceptions::CMSCRLNotSet, 227

rpki::exceptions::CMSVerificationFailed, 228
rpki::exceptions::DBConsistancyError, 229
rpki::exceptions::DERObjectConversionError, 230
rpki::exceptions::DuplicateObject, 231
rpki::exceptions::EmptyPEM, 232
rpki::exceptions::EmptyROAPrefixList, 233
rpki::exceptions::ForbiddenURI, 234
rpki::exceptions::HandleTranslationError, 235
rpki::exceptions::HTTPRequestFailed, 236
rpki::exceptions::HTTPSBadVersion, 237
rpki::exceptions::HTTPSClientAborted, 238
rpki::exceptions::HTTPSUnexpectedState, 239
rpki::exceptions::MissingCMSCRL, 240
rpki::exceptions::MissingCMSEEcert, 241
rpki::exceptions::MultipleTLSEECert, 242
rpki::exceptions::MustBePrefix, 243
rpki::exceptions::NoActiveCA, 244
rpki::exceptions::NoCoveringCertForROA, 245
rpki::exceptions::NoObjectAtURI, 246
rpki::exceptions::NotACertificateChain, 247
rpki::exceptions::NotFound, 248
rpki::exceptions::NotImplementedYet, 249
rpki::exceptions::NotInDatabase, 250
rpki::exceptions::ReceivedTLSCACert, 251
rpki::exceptions::RPKI_Exception, 253
rpki::exceptions::ServerShuttingDown, 254
rpki::exceptions::SKIMismatch, 255
rpki::exceptions::SubprocessError, 256
rpki::exceptions::TLSValidationError, 257
rpki::exceptions::UnexpectedCMSCerts, 259
rpki::exceptions::UnexpectedCMSCRLs, 260
rpki::exceptions::UnparsableCMSDER, 261
rpki::exceptions::UpstreamError, 262
rpki::exceptions::WrongEContentType, 263
rpki::https
build_https_ta_cache, 85
client, 85
client_queues, 86
debug_http, 86
debug_tls_certs, 86
default_client_timeout, 86
default_http_version, 86
default_server_timeout, 86
log_method, 85
rpki_content_type, 87
server, 85
supported_address_families, 87
want_persistent_client, 87
want_persistent_server, 87
rpki::https::caller, 264
__call__, 265
__init__, 265
client_cert, 265
client_key, 265
debug, 266
proto, 266
server_cert, 266
server_ta, 266
url, 266
rpki::https::http_client, 266
__init__, 268
af, 271
cert, 271
expect_close, 271
handle_close, 268
handle_connect, 269
handle_error, 269
handle_message, 269
handle_no_content_length, 269
handle_timeout, 270
hostport, 271

key, 271
parse_type, 271
queue, 272
retry_read, 272
retry_write, 272
send_request, 270
set_state, 270
start, 270
state, 272
ta, 272
timeout, 272
tls, 272
tls_connect, 270
rpki::https::http_listener, 273
__init__, 274
cert, 275
dynamic_ta, 275
handle_accept, 274
handle_error, 274
handlers, 275
key, 275
log, 275
ta, 275
rpki::https::http_message, 276
__init__, 277
__str__, 277
body, 279
format, 277
headers, 279
normalize_headers, 278
parse_from_wire, 278
parse_version, 278
persistent, 278
software_name, 279
version, 279
rpki::https::http_queue, 279
__init__, 281
cert, 282
client, 282
detach, 281
hostport, 283
key, 283
log, 283
queue, 283
request, 281
restart, 282
return_result, 282
send_request, 282
ta, 283
rpki::https::http_request, 283
__init__, 285
callback, 286
cmd, 286
errback, 286
format_first_line, 285
parse_first_line, 285
path, 286
retried, 286
rpki::https::http_response, 286
__init__, 288
code, 288
format_first_line, 288
parse_first_line, 288
reason, 288
rpki::https::http_server, 289
__init__, 291
expect_close, 293
find_handler, 291
handle_message, 291
handle_no_content_length, 292
handlers, 293
parse_type, 293
retry_read, 293
retry_write, 293
send_error, 292
send_message, 292
send_reply, 292
timeout, 294
tls, 294
tls_accept, 292
rpki::https::http_stream, 294
__init__, 297
buffer, 302
chunk_body, 297
chunk_discard_crlf, 297
chunk_discard_trailer, 297
chunk_handler, 302
chunk_header, 297
close, 297
collect_incoming_data, 298
found_terminator, 298
get_buffer, 298

handle_body, 298
handle_close, 299
handle_error, 299
handle_read, 299
handle_timeout, 299
handle_write, 300
initiate_send, 300
log, 302
log_cert, 300
msg, 302
readable, 300
recv, 300
restart, 301
retry_read, 302
retry_write, 302
send, 301
timer, 302
tls, 303
update_timeout, 301
writeable, 301
rpki::ipaddrs::v4addr, 303
__new__, 304
__str__, 304
bits, 305
from_bytes, 304
to_bytes, 304
rpki::ipaddrs::v6addr, 305
__new__, 307
__str__, 307
bits, 307
from_bytes, 307
to_bytes, 307
rpki::left_right
enforce_strict_up_down_xml_-sender, 90
rpki::left_right::bsc_elt, 308
attributes, 311
booleans, 311
children, 310
element_name, 312
elements, 312
handles, 312
parents, 310
pkcs10_request, 312
private_key_id, 312
repositories, 311
serve_pre_save_hook, 311
signing_cert, 312
signing_cert_crl, 313
sql_template, 313
rpki::left_right::child_elt, 313
attributes, 317
booleans, 317
bpki_cert, 317
bpki_glue, 317
ca_from_class_name, 315
child_certs, 315
clear_https_ta_cache, 317
element_name, 317
elements, 318
endElement, 316
handles, 318
parents, 316
serve_destroy_hook, 316
serve_post_save_hook, 316
serve_up_down, 316
sql_template, 318
rpki::left_right::cms_msg, 318
encoding, 320
saxify, 320
schema, 320
rpki::left_right::data_elt, 320
bsc, 322
handles, 324
make_reply_clone_hook, 322
self, 322
self_handle, 324
self_id, 324
serve_fetch_all, 323
serve_fetch_handle, 323
serve_fetch_one_maybe, 323
serve_pre_save_hook, 323
rpki::left_right::left_right_namespace, 324
nsmap, 325
xmlns, 325
rpki::left_right::list_published_objects_-elt, 326
attributes, 329
element_name, 329
make_reply, 328
obj, 329

serve_dispatch, 328
text_attribute, 329
rpki::left_right::list_received_resources_-elt, 329
attributes, 331
element_name, 331
make_reply, 331
serve_dispatch, 331
rpki::left_right::list_resources_elt, 332
asn, 335
attributes, 335
element_name, 335
ipv4, 335
ipv6, 335
startElement, 334
toXML, 334
valid_until, 335
rpki::left_right::list_roa_requests_elt, 336
attributes, 337
element_name, 337
ipv4, 338
ipv6, 338
startElement, 337
rpki::left_right::msg, 338
pdus, 340
serve_top_level, 340
version, 340
rpki::left_right::parent_elt, 341
attributes, 345
booleans, 345
bpki_cms_cert, 345
bpki_cms_glue, 345
bpki_https_cert, 346
bpki_https_glue, 346
cas, 343
element_name, 346
elements, 346
handles, 346
query_up_down, 343
repository, 344
serve_post_save_hook, 344
serve_rekey, 344
serve_revoke, 344
serve_revoke_forgotten, 344
sql_template, 346
rpki::left_right::report_error_elt, 347
attributes, 350
element_name, 350
error_code, 350
error_text, 350
from_exception, 349
self_handle, 350
tag, 350
text_attribute, 350
rpki::left_right::repository_elt, 351
attributes, 354
bpki_cert, 354
bpki_glue, 354
call_pubd, 353
default_pubd_handler, 353
element_name, 354
elements, 355
handles, 355
parents, 354
sql_template, 355
rpki::left_right::sax_handler, 355
name, 357
pdu, 357
version, 357
rpki::left_right::self_elt, 357
attributes, 364
booleans, 364
bpki_cert, 364
bpki_glue, 364
bscs, 360
children, 360
client_poll, 360
crl_interval, 365
cron, 360
element_name, 365
elements, 365
handles, 365
parents, 360
regen_margin, 365
regenerate_crls_and_manifests, 361
repositories, 361
roas, 361
serve_fetch_all, 361
serve_fetch_handle, 362
serve_fetch_one_maybe, 362
serve_post_save_hook, 362
serve_publish_world_now, 362

serve_rekey, 363
serve_revoke, 363
serve_revoke_forgotten, 363
serve_run_now, 363
sql_template, 365
update_children, 363
update_roas, 364
use_hsm, 366
rpki::log
debug, 92
enable_trace, 92
error, 92
info, 92
init, 91
note, 93
pid, 93
set_trace, 91
tag, 93
trace, 92
traceback, 92
use_syslog, 93
warn, 93
rpki::log::logger, 366
__call__, 367
__init__, 367
priority, 367
rpki::manifest::FileAndHash, 368
__init__, 369
file, 369
hash, 369
rpki::manifest::FilesAndHashes, 369
__init__, 370
rpki::manifest::Manifest, 371
__init__, 372
explicitVersion, 372
fileHashAlg, 372
fileList, 372
manifestNumber, 372
nextUpdate, 372
thisUpdate, 373
version, 373
rpki::myrpki
allow_incomplete, 97
b64_equal, 96
csv_writer, 96
etree_post_read, 96
etree_pre_write, 96
etree_read, 97
etree_validate, 97
etree_write, 97
namespace, 98
namespaceQName, 98
PEMElement, 97
version, 98
whine, 98
rpki::myrpki::CA, 373
__init__, 375
bsc, 375
cer, 378
cfg, 378
cms_xml_sign, 376
cms_xml_verify, 376
crl, 378
crlnum, 378
dir, 378
ee, 376
env, 379
fxcert, 376
index, 379
key, 379
openssl, 379
path_restriction, 379
req, 379
run_ca, 376
run_dgst, 377
run_openssl, 377
run_req, 377
serial, 379
setup, 377
touch_file, 377
xcert, 378
rpki::myrpki::child, 380
__init__, 382
__repr__, 382
add, 382
asns, 383
bpki_certificate, 383
handle, 383
v4, 383
v4re, 383
v6, 383
v6re, 384

validity, 384
xml, 382
rpki::myrpki::children, 384
add, 385
from_csv, 386
xml, 386
rpki::myrpki::comma_set, 386
__str__, 387
rpki::myrpki::csv_reader, 388
__init__, 389
__iter__, 389
columns, 389
comment_characters, 389
file, 389
filename, 390
min_columns, 390
rpki::myrpki::EntityDB, 390
__call__, 392
__init__, 392
dir, 392
iterate, 392
rpki::myrpki::main, 392
__init__, 394
bpki_resources, 397
bpki_servers, 397
cfg, 397
cfg_file, 397
completedefault, 398
configure_resources_main, 394
do_configure_child, 395
do_configure_daemons, 395
do_configure_parent, 395
do_configure_publication_client, 396
do_configure_repository, 396
do_configure_resources, 396
do_initialize, 396
entitydb, 398
handle, 398
help_overview, 397
histfile, 398
prompt, 398
pubd_contact_info, 398
read_config, 397
rsync_module, 398
rsync_server, 399
run_pubd, 399
run_rootd, 399
run_rpkid, 399
show_xml, 399
rpki::myrpki::parent, 399
__init__, 401
__repr__, 401
add, 401
bpki_cms_certificate, 402
bpki_https_certificate, 402
handle, 402
myhandle, 402
service_uri, 402
sia_base, 402
xml, 401
rpki::myrpki::parents, 402
add, 403
from_csv, 404
xml, 404
rpki::myrpki::repositories, 404
add, 405
from_csv, 406
xml, 406
rpki::myrpki::repository, 406
__init__, 408
__repr__, 408
add, 408
bpki_certificate, 408
handle, 408
service_uri, 409
xml, 408
rpki::myrpki::roa_request, 409
__init__, 411
__repr__, 411
add, 411
asn, 412
group, 412
v4, 412
v4re, 412
v6, 412
v6re, 412
xml, 411
rpki::myrpki::roa_requests, 413
add, 413
from_csv, 414
xml, 414

rpki::oids
name2oid, 99
oid2name, 99
rpki::publication::certificate_elt, 414
element_name, 416
payload_type, 416
rpki::publication::client_elt, 416
attributes, 419
base_uri, 419
bpki_cert, 420
bpki_glue, 420
check_allowed_uri, 418
clear_https_ta_cache, 420
element_name, 420
elements, 420
endElement, 418
serve_fetch_all, 419
serve_fetch_one_maybe, 419
serve_post_save_hook, 419
sql_template, 420
rpki::publication::cms_msg, 421
encoding, 423
saxify, 423
schema, 423
rpki::publication::config_elt, 423
attributes, 426
config_id, 426
element_name, 427
elements, 427
fetch, 425
serve_fetch_one_maybe, 425
serve_set, 426
sql_template, 427
startElement, 426
wired_in_config_id, 427
rpki::publication::control_elt, 427
serve_dispatch, 430
rpki::publication::crl_elt, 430
element_name, 432
payload_type, 432
rpki::publication::manifest_elt, 432
element_name, 434
payload_type, 434
rpki::publication::msg, 434
pdus, 436
serve_top_level, 436
version, 436
rpki::publication::publication_-namespace, 437
nsmap, 438
xmlns, 438
rpki::publication::publication_object_elt, 438
attributes, 442
endElement, 440
make_publish, 440
make_withdraw, 441
payload, 442
payload_type, 442
raise_if_error, 441
serve_dispatch, 441
serve_publish, 441
serve_withdraw, 441
toXML, 442
uri_to_filename, 442
rpki::publication::report_error_elt, 443
__str__, 445
attributes, 446
element_name, 446
error_code, 446
error_text, 446
from_exception, 445
raise_if_error, 446
tag, 447
text_attribute, 447
rpki::publication::roa_elt, 447
element_name, 449
payload_type, 449
rpki::publication::sax_handler, 449
name, 451
pdu, 451
version, 451
rpki::relaxng
left_right, 101
publication, 101
up_down, 101
rpki::resource_set
_bs2long, 103
_long2bs, 103
_rsplit, 104
inherit_token, 104
test1, 104

test2, 104
rpki::resource_set::resource_bag, 451
__eq__, 453
__init__, 453
__ne__, 453
__str__, 454
asn, 455
empty, 454
from_rfc3779_tuples, 454
intersection, 454
oversized, 454
undersized, 454
union, 455
v4, 455
v6, 455
valid_until, 455
rpki::resource_set::resource_range, 456
__cmp__, 457
__init__, 457
max, 457
min, 457
rpki::resource_set::resource_range_as, 458
__str__, 459
datum_type, 459
min, 460
to_rfc3779_tuple, 459
rpki::resource_set::resource_range_ip, 460
__str__, 462
_prefixlen, 462
make_prefix, 462
to_rfc3779_tuple, 462
rpki::resource_set::resource_range_ipv4, 463
datum_type, 465
rpki::resource_set::resource_range_ipv6, 465
datum_type, 467
rpki::resource_set::resource_set, 467
__init__, 469
__str__, 469
_comm, 469
contains, 470
difference, 470
from_sql, 470
inherit, 471
intersection, 470
issubset, 470
issuperset, 471
symmetric_difference, 471
union, 471
rpki::resource_set::resource_set_as, 472
inherit, 474
parse_rfc3779_tuple, 473
parse_str, 473
range_type, 474
to_rfc3779_tuple, 473
rpki::resource_set::resource_set_ip, 474
inherit, 477
parse_rfc3779_tuple, 476
parse_str, 476
to_rfc3779_tuple, 476
rpki::resource_set::resource_set_ipv4, 477
afi, 479
range_type, 479
rpki::resource_set::resource_set_ipv6, 479
afi, 481
range_type, 481
rpki::resource_set::roa_prefix, 481
__cmp__, 483
__init__, 483
__str__, 483
max, 483
max_prefixlen, 484
min, 484
prefix, 484
prefixlen, 485
to_resource_range, 484
to_roa_tuple, 484
rpki::resource_set::roa_prefix_ipv4, 485
range_type, 487
rpki::resource_set::roa_prefix_ipv6, 487
range_type, 489
rpki::resource_set::roa_prefix_set, 489
__init__, 491
__str__, 491
from_sql, 491
parse_str, 491
to_resource_set, 491

to_roa_tuple, 492
rpki::resource_set::roa_prefix_set_ipv4, 492
prefix_type, 494
resource_set_type, 494
rpki::resource_set::roa_prefix_set_ipv6, 494
prefix_type, 496
resource_set_type, 496
rpki::roa::ROAIPAddress, 496
__init__, 497
address, 498
maxLength, 498
rpki::roa::ROAIPAddresses, 498
__init__, 499
rpki::roa::ROAIPAddressFamilies, 499
__init__, 500
rpki::roa::ROAIPAddressFamily, 500
__init__, 501
addresses, 502
addressFamily, 502
rpki::roa::RouteOriginAttestation, 502
__init__, 503
asID, 503
explicitVersion, 503
ipAddrBlocks, 503
version, 503
rpki::rpki_engine::ca_detail_obj, 504
activate, 507
ca, 507
ca_cert_uri, 511
ca_id, 511
child_certs, 507
create, 507
crl_published, 511
crl_published_callback, 507
crl_uri, 507
crl_uri_tail, 508
delete, 508
gctx, 511
generate_crl, 508
generate_manifest, 508
generate_manifest_cert, 508
issue, 509
issue_ee, 509
latest_ca_cert, 511
latest_crl, 511
latest_manifest, 512
latest_manifest_cert, 512
manifest_private_key_id, 512
manifest_public_key, 512
manifest_published, 512
manifest_published_callback, 509
manifest_uri, 509
nextUpdate, 512
private_key_id, 512
public_key, 513
revoke, 509
revoked_certs, 510
roas, 510
sql_decode, 510
sql_template, 513
state, 513
update, 510
rpki::rpki_engine::ca_obj, 513
ca_details, 515
check_for_updates, 515
construct_sia_uri, 516
create, 516
delete, 516
fetch_active, 516
fetch_deprecated, 517
fetch_issue_response_candidates, 517
fetch_pending, 517
fetch_revoked, 517
gctx, 519
last_crl_sn, 519
last_issued_sn, 519
last_manifest_sn, 519
next_crl_number, 517
next_manifest_number, 518
next_serial_number, 518
parent, 518
parent_id, 519
parent_resource_class, 519
rekey, 518
revoke, 518
sia_uri, 520
sql_template, 520
rpki::rpki_engine::child_cert_obj, 520
__init__, 522

ca_detail, 522
ca_detail_id, 524
cert, 524
child, 522
child_id, 524
fetch, 523
gctx, 524
published, 524
published_callback, 523
reissue, 523
revoke, 523
sql_template, 525
uri, 523
uri_tail, 524
rpki::rpki_engine::publication_queue, 525
__init__, 527
_add, 527
call_pubd, 527
handlers, 528
msgs, 528
publish, 527
replace, 528
repositories, 528
uris, 528
withdraw, 528
rpki::rpki_engine::revoked_cert_obj, 529
__init__, 530
ca_detail, 530
ca_detail_id, 531
expires, 531
gctx, 531
revoke, 530
revoked, 531
serial, 531
sql_template, 531
rpki::rpki_engine::roa_obj, 532
__init__, 534
asn, 537
ca_detail, 534
ca_detail_id, 537
cert, 537
gctx, 538
generate, 535
ipv4, 538
ipv6, 538
published, 538
published_callback, 535
regenerate, 535
revoke, 535
roa, 538
self, 536
self_id, 538
sql_delete_hook, 536
sql_fetch_hook, 536
sql_insert_hook, 536
sql_template, 538
update, 537
uri, 537
uri_tail, 537
rpki::rpki_engine::rpkid_context, 539
__init__, 542
bpki_ta, 544
build_https_ta_cache, 542
checkpoint, 542
clear_https_ta_cache, 542
cron, 542
cron_keepalive, 544
cron_period, 544
cron_timeout, 544
cron_timer, 544
cronjob_handler, 542
https_server_host, 545
https_server_port, 545
https_ta_cache, 545
initial_delay, 545
irbe_cert, 545
irdb_cert, 545
irdb_query, 543
irdb_query_child_resources, 543
irdb_query_roa_requests, 543
irdb_url, 545
left_right_handler, 543
publication_kludge_base, 546
rpkid_cert, 546
rpkid_key, 546
sql, 546
start_cron, 543
up_down_handler, 544
up_down_url_regexp, 546
use_internal_cron, 546
rpki::sql::session, 547

__init__, 549
_exceptions_enabled, 550
_wrap_execute, 549
assert_pristine, 549
cache, 551
cache_clear, 549
close, 549
connect, 549
cur, 551
database, 551
db, 551
dirty, 551
execute, 549
executemany, 550
fetchall, 550
lastrowid, 550
password, 551
ping, 550
sweep, 550
username, 551
rpki::sql::sql_persistent, 552
gctx, 558
sql_debug, 558
sql_decode, 554
sql_delete, 555
sql_delete_hook, 555
sql_deleted, 558
sql_encode, 555
sql_fetch, 555
sql_fetch_all, 556
sql_fetch_hook, 556
sql_fetch_where, 556
sql_fetch_where1, 556
sql_in_db, 559
sql_init, 556
sql_insert_hook, 557
sql_is_dirty, 557
sql_mark_clean, 557
sql_mark_deleted, 557
sql_mark_dirty, 557
sql_store, 558
sql_update_hook, 558
rpki::sql::template, 559
__init__, 561
columns, 561
delete, 561
index, 561
insert, 561
map, 562
select, 562
table, 562
update, 562
rpki::sundial
_cast, 108
now, 108
test, 109
rpki::sundial::datetime, 562
__add__, 564
__radd__, 564
__rsub__, 564
__str__, 565
__sub__, 565
earlier, 565
from_sql, 565
fromASN1tuple, 565
fromdatetime, 565
fromGeneralizedTime, 566
fromUTCTime, 566
fromXMLtime, 566
later, 566
PKIX_threshhold, 568
to_sql, 566
toASN1tuple, 567
toGeneralizedTime, 567
totimestamp, 567
toUTCTime, 567
toXMLtime, 567
rpki::sundial::timedelta, 568
__abs__, 571
__add__, 571
__div__, 571
__floordiv__, 571
__mul__, 571
__neg__, 571
__pos__, 571
__radd__, 571
__rdiv__, 572
__rfloordiv__, 572
__rmul__, 572
__rsub__, 572
__sub__, 572
convert_to_seconds, 572

fromtimedelta, 572
parse, 573
regexp, 573
years_to_seconds, 573
rpki::up_down
nsmap, 110
xmlns, 110
rpki::up_down::base_elt, 574
check_response, 575
endElement, 575
make_b64elt, 575
make_elt, 575
serve_pdu, 576
startElement, 576
rpki::up_down::certificate_elt, 576
cert, 579
cert_url, 579
endElement, 578
req_resource_set_as, 579
req_resource_set_ipv4, 579
req_resource_set_ipv6, 579
startElement, 578
toXML, 578
rpki::up_down::class_elt, 579
__init__, 581
cert_url, 582
certs, 582
class_name, 582
endElement, 581
from_resource_bag, 581
issuer, 583
resource_set_as, 583
resource_set_ipv4, 583
resource_set_ipv6, 583
resource_set_notafter, 583
startElement, 582
suggested_sia_head, 583
to_resource_bag, 582
toXML, 582
rpki::up_down::class_response_syntax, 584
__init__, 585
classes, 586
startElement, 585
toXML, 585
rpki::up_down::cms_msg, 586
encoding, 588
saxify, 588
schema, 588
rpki::up_down::error_response_pdu, 588
__init__, 590
check_response, 590
codes, 591
description, 591
endElement, 590
exceptions, 591
status, 591
toXML, 591
rpki::up_down::issue_pdu, 592
class_name, 595
endElement, 594
pkcs10, 595
query, 594
req_resource_set_as, 595
req_resource_set_ipv4, 595
req_resource_set_ipv6, 595
serve_pdu, 594
startElement, 594
toXML, 595
rpki::up_down::issue_response_pdu, 596
check_response, 598
rpki::up_down::list_pdu, 598
query, 600
serve_pdu, 600
toXML, 600
rpki::up_down::list_response_pdu, 601
rpki::up_down::message_pdu, 602
__str__, 604
log_query, 604
make_query, 604
name2type, 606
payload, 606
recipient, 606
sender, 606
serve_error, 605
serve_top_level, 605
startElement, 605
toXML, 605
type, 606
type2name, 606
version, 607
rpki::up_down::multi_uri, 607

__init__, 608
__str__, 609
rsync, 609
rpki::up_down::revoke_pdu, 609
class_name, 612
get_SKI, 611
query, 611
serve_pdu, 611
ski, 612
rpki::up_down::revoke_response_pdu, 612
rpki::up_down::revoke_syntax, 614
class_name, 615
ski, 615
startElement, 615
toXML, 615
rpki::up_down::sax_handler, 616
name, 618
pdu, 618
version, 618
rpki::x509
_find_xia_uri, 112
calculate_SKI, 112
POWify_OID, 112
rpki::x509::CMS_object, 618
content, 622
debug_cms_certs, 622
DER, 623
dump_on_verify_failure, 623
econtent_oid, 623
extract, 621
formats, 623
get_content, 621
get_DER, 621
get_POW, 621
other_clear, 623
pem_converter, 624
POW, 624
print_on_der_error, 624
require_crls, 624
set_content, 622
sign, 622
verify, 622
rpki::x509::CRL, 625
DER, 628
formats, 628
generate, 626
get_DER, 626
get_POW, 627
get_POWpkix, 627
getIssuer, 627
getNextUpdate, 627
getThisUpdate, 627
pem_converter, 628
POW, 628
POWpkix, 628
rpki::x509::DeadDrop, 629
__init__, 630
dump, 630
maildir, 630
pid, 630
rpki::x509::DER_CMS_object, 631
content, 632
decode, 632
encode, 632
rpki::x509::DER_object, 633
__cmp__, 635
__init__, 635
clear, 635
DER, 640
dumpasn1, 635
empty, 635
formats, 640
from_sql, 636
gAKI, 636
get_3779resources, 636
get_AIA, 636
get_aia_uri, 636
get_AKI, 637
get_Base64, 637
get_basicConstraints, 637
get_DER, 637
get_PEM, 637
get_SIA, 638
get_sia_directory_uri, 638
get_sia_manifest_uri, 638
get_SKI, 638
gSKI, 638
hAKI, 639
hSKI, 639
is_CA, 639
other_clear, 640

pem_converter, 640
set, 639
to_sql, 639
rpki::x509::PEM_converter, 641
__init__, 642
b, 643
e, 643
looks_like_PEM, 642
to_DER, 642
to_PEM, 642
rpki::x509::PKCS10, 643
check_valid_rpki, 645
create, 645
create_ca, 645
DER, 646
formats, 646
get_DER, 646
get_POWpkix, 646
getPublicKey, 646
pem_converter, 647
POWpkix, 647
rpki::x509::ROA, 647
build, 649
content_class, 649
econtent_oid, 649
pem_converter, 649
rpki::x509::RSA, 650
DER, 653
formats, 653
generate, 652
get_DER, 652
get_POW, 652
get_public_DER, 653
get_RSApublic, 653
get_SKI, 653
pem_converter, 654
POW, 654
rpki::x509::RSApublic, 654
DER, 657
formats, 657
get_DER, 656
get_POW, 656
get_SKI, 656
pem_converter, 657
POW, 657
rpki::x509::SignedManifest, 658
build, 659
content_class, 660
econtent_oid, 660
getNextUpdate, 659
getThisUpdate, 659
pem_converter, 660
rpki::x509::X509, 660
cross_certify, 662
DER, 665
expired, 663
formats, 665
get_DER, 663
get_POW, 663
get_POWpkix, 663
getIssuer, 663
getNotAfter, 663
getNotBefore, 664
getPublicKey, 664
getSerial, 664
getSubject, 664
issue, 664
normalize_chain, 665
pem_converter, 665
POW, 666
POWpkix, 666
rpki::x509::XML_CMS_object, 666
content, 670
decode, 668
dump_inbound_cms, 670
dump_outbound_cms, 670
dump_to_disk, 668
econtent_oid, 670
encode, 668
pretty_print_content, 669
schema_check, 669
unwrap, 669
wrap, 669
rpki::xml_utils::base_elt, 670
__str__, 672
attributes, 674
booleans, 674
elements, 674
endElement, 672
make_b64elt, 673
make_elt, 673
make_pdu, 673

read_attrs, 673
startElement, 673
toXML, 674
rpki::xml_utils::data_elt, 675
endElement, 677
make_reply, 677
make_reply_clone_hook, 677
serve_create, 678
serve_destroy, 678
serve_destroy_hook, 678
serve_dispatch, 678
serve_fetch_one, 678
serve_get, 679
serve_list, 679
serve_post_save_hook, 679
serve_pre_save_hook, 679
serve_set, 679
toXML, 680
unimplemented_control, 680
rpki::xml_utils::msg, 680
__str__, 682
endElement, 682
is_query, 682
is_reply, 682
query, 682
reply, 683
startElement, 683
toXML, 683
type, 683
version, 683
rpki::xml_utils::sax_handler, 684
__init__, 685
characters, 685
create_top_level, 686
endElement, 686
endElementNS, 686
result, 687
saxify, 686
stack, 687
startElement, 686
startElementNS, 687
text, 687
rpki::xml_utils::text_elt, 688
endElement, 689
text_attribute, 689
toXML, 689
rpki_base_uri
rootd, 73
rpki_class_name
rootd, 74
rpki_content_type
rpki::https, 87
rpki_engine.py(3107), 706
rpki_root_cert
rootd, 74
rpki_root_cert_file
rootd, 74
rpki_root_cert_uri
rootd, 74
rpki_root_crl
rootd, 74
rpki_root_dir
rootd, 74
rpki_root_key
rootd, 74
rpki_root_manifest
rootd, 75
rpki_subject_cert
rootd, 75
rpki_subject_lifetime
rootd, 75
rpki_subject_pkcs10
rootd, 75
rpki_subject_regen
rootd, 75
rpkid, 113
cfg_file, 115
main, 114
profile, 115
rpkid.py(2913), 707
rpkid_cert
irdbd, 66
rpki::rpki_engine::rpkid_context, 546
rpkid_key
rpki::rpki_engine::rpkid_context, 546
rsync
rpki::up_down::multi_uri, 609
rsync_module
rpki::myrpki::main, 398
rsync_server

rpki::myrpki::main, 399
run_ca
rpki::myrpki::CA, 376
run_debug
rpki::async::timer, 197
run_deferred
rpki::async, 78
run_dgst
rpki::myrpki::CA, 377
run_openssl
rpki::myrpki::CA, 377
run_pubd
rpki::myrpki::main, 399
run_req
rpki::myrpki::CA, 377
run_rootd
rpki::myrpki::main, 399
run_rpkid
rpki::myrpki::main, 399
runq
rpki::async::timer, 195

saxify
irbe_cli::left_right_cms_msg, 136
irbe_cli::publication_cms_msg, 151
rootd::cms_msg, 173
rpki::left_right::cms_msg, 320
rpki::publication::cms_msg, 423
rpki::up_down::cms_msg, 588
rpki::xml_utils::sax_handler, 686
schema
rpki::left_right::cms_msg, 320
rpki::publication::cms_msg, 423
rpki::up_down::cms_msg, 588
schema_check
rpki::x509::XML_CMS_object, 669
seconds_until_wakeup
rpki::async::timer, 195
select
rpki::sql::template, 562
self
rpki::left_right::data_elt, 322
rpki::rpki_engine::roa_obj, 536
self_handle
rpki::left_right::data_elt, 324
rpki::left_right::report_error_elt, 350
self_id
rpki::left_right::data_elt, 324
rpki::rpki_engine::roa_obj, 538
send
rpki::https::http_stream, 301
send_error
rpki::https::http_server, 292
send_message
rpki::https::http_server, 292
send_reply
rpki::https::http_server, 292
send_request
rpki::https::http_client, 270
rpki::https::http_queue, 282
sender
rpki::up_down::message_pdu, 606
Sequence, 690
SequenceOf, 690
serial
rpki::myrpki::CA, 379
rpki::rpki_engine::revoked_cert_obj, 531
serve_create
rpki::xml_utils::data_elt, 678
serve_destroy
rpki::xml_utils::data_elt, 678
serve_destroy_hook
rpki::left_right::child_elt, 316
rpki::xml_utils::data_elt, 678
serve_dispatch
rpki::left_right::list_published_-objects_elt, 328
rpki::left_right::list_received_-resources_elt, 331
rpki::publication::control_elt, 430
rpki::publication::publication_-object_elt, 441
rpki::xml_utils::data_elt, 678
serve_error
rpki::up_down::message_pdu, 605
serve_fetch_all
rpki::left_right::data_elt, 323
rpki::left_right::self_elt, 361
rpki::publication::client_elt, 419
serve_fetch_handle
rpki::left_right::data_elt, 323

rpki::left_right::self_elt, 362
serve_fetch_one
rpki::xml_utils::data_elt, 678
serve_fetch_one_maybe
rpki::left_right::data_elt, 323
rpki::left_right::self_elt, 362
rpki::publication::client_elt, 419
rpki::publication::config_elt, 425
serve_get
rpki::xml_utils::data_elt, 679
serve_list
rpki::xml_utils::data_elt, 679
serve_pdu
rootd::issue_pdu, 175
rootd::list_pdu, 177
rootd::revoke_pdu, 181
rpki::up_down::base_elt, 576
rpki::up_down::issue_pdu, 594
rpki::up_down::list_pdu, 600
rpki::up_down::revoke_pdu, 611
serve_post_save_hook
rpki::left_right::child_elt, 316
rpki::left_right::parent_elt, 344
rpki::left_right::self_elt, 362
rpki::publication::client_elt, 419
rpki::xml_utils::data_elt, 679
serve_pre_save_hook
rpki::left_right::bsc_elt, 311
rpki::left_right::data_elt, 323
rpki::xml_utils::data_elt, 679
serve_publish
rpki::publication::publication_-object_elt, 441
serve_publish_world_now
rpki::left_right::self_elt, 362
serve_rekey
rpki::left_right::parent_elt, 344
rpki::left_right::self_elt, 363
serve_revoke
rpki::left_right::parent_elt, 344
rpki::left_right::self_elt, 363
serve_revoke_forgotten
rpki::left_right::parent_elt, 344
rpki::left_right::self_elt, 363
serve_run_now
rpki::left_right::self_elt, 363
serve_set
rpki::publication::config_elt, 426
rpki::xml_utils::data_elt, 679
serve_top_level
rpki::left_right::msg, 340
rpki::publication::msg, 436
rpki::up_down::message_pdu, 605
serve_up_down
rpki::left_right::child_elt, 316
serve_withdraw
rpki::publication::publication_-object_elt, 441
server
rpki::https, 85
server_cert
irdbd, 66
rootd, 75
rpki::https::caller, 266
server_ta
rpki::https::caller, 266
service_uri
rpki::myrpki::parent, 402
rpki::myrpki::repository, 409
set, 690
rpki::async::timer, 195
rpki::x509::DER_object, 639
set_content
rpki::x509::CMS_object, 622
set_errback
rpki::async::timer, 196
set_global_flags
rpki::config::parser, 206
set_handler
rpki::async::timer, 196
set_state
rpki::https::http_client, 270
set_subject_cert
rootd, 71
set_subject_pkcs10
rootd, 71
set_trace
rpki::log, 91
setup
rpki::myrpki::CA, 377
show_xml
rpki::myrpki::main, 399

sia_base
rpki::myrpki::parent, 402
sia_uri
rpki::rpki_engine::ca_obj, 520
sign
rpki::x509::CMS_object, 622
signing_cert
irbe_cli::bsc_elt, 119
rpki::left_right::bsc_elt, 312
signing_cert_crl
irbe_cli::bsc_elt, 119
rpki::left_right::bsc_elt, 313
ski
rpki::up_down::revoke_pdu, 612
rpki::up_down::revoke_syntax, 615
software_name
rpki::https::http_message, 279
sql
pubd::pubd_context, 171
rpki::rpki_engine::rpkid_context, 546
sql.py(2895), 707
sql_debug
rpki::sql::sql_persistent, 558
sql_decode
rpki::rpki_engine::ca_detail_obj, 510
rpki::sql::sql_persistent, 554
sql_delete
rpki::sql::sql_persistent, 555
sql_delete_hook
rpki::rpki_engine::roa_obj, 536
rpki::sql::sql_persistent, 555
sql_deleted
rpki::sql::sql_persistent, 558
sql_encode
rpki::sql::sql_persistent, 555
sql_fetch
rpki::sql::sql_persistent, 555
sql_fetch_all
rpki::sql::sql_persistent, 556
sql_fetch_hook
rpki::rpki_engine::roa_obj, 536
rpki::sql::sql_persistent, 556
sql_fetch_where
rpki::sql::sql_persistent, 556
sql_fetch_where1
rpki::sql::sql_persistent, 556
sql_in_db
rpki::sql::sql_persistent, 559
sql_init
rpki::sql::sql_persistent, 556
sql_insert_hook
rpki::rpki_engine::roa_obj, 536
rpki::sql::sql_persistent, 557
sql_is_dirty
rpki::sql::sql_persistent, 557
sql_mark_clean
rpki::sql::sql_persistent, 557
sql_mark_deleted
rpki::sql::sql_persistent, 557
sql_mark_dirty
rpki::sql::sql_persistent, 557
sql_store
rpki::sql::sql_persistent, 558
sql_template
rpki::left_right::bsc_elt, 313
rpki::left_right::child_elt, 318
rpki::left_right::parent_elt, 346
rpki::left_right::repository_elt, 355
rpki::left_right::self_elt, 365
rpki::publication::client_elt, 420
rpki::publication::config_elt, 427
rpki::rpki_engine::ca_detail_obj, 513
rpki::rpki_engine::ca_obj, 520
rpki::rpki_engine::child_cert_obj, 525
rpki::rpki_engine::revoked_cert_obj, 531
rpki::rpki_engine::roa_obj, 538
sql_update_hook
rpki::sql::sql_persistent, 558
stack
rpki::xml_utils::sax_handler, 687
start
rpki::https::http_client, 270
start_cron
rpki::rpki_engine::rpkid_context, 543
startElement

rpki::left_right::list_resources_elt, 334
rpki::left_right::list_roa_requests_-elt, 337
rpki::publication::config_elt, 426
rpki::up_down::base_elt, 576
rpki::up_down::certificate_elt, 578
rpki::up_down::class_elt, 582
rpki::up_down::class_response_-syntax, 585
rpki::up_down::issue_pdu, 594
rpki::up_down::message_pdu, 605
rpki::up_down::revoke_syntax, 615
rpki::xml_utils::base_elt, 673
rpki::xml_utils::msg, 683
rpki::xml_utils::sax_handler, 686
startElementNS
rpki::xml_utils::sax_handler, 687
startup_msg
irdbd, 66
state
rpki::https::http_client, 272
rpki::rpki_engine::ca_detail_obj, 513
status
rpki::up_down::error_response_pdu, 591
suggested_sia_head
rpki::up_down::class_elt, 583
sundial.py(3191), 707
supported_address_families
rpki::https, 87
sweep
rpki::sql::session, 550
symmetric_difference
rpki::resource_set::resource_set, 471

ta
rpki::https::http_client, 272
rpki::https::http_listener, 275
rpki::https::http_queue, 283
table
rpki::sql::template, 562
tag
rpki::left_right::report_error_elt, 350
rpki::log, 93
rpki::publication::report_error_elt, 447
test
rpki::sundial, 109
test1
rpki::resource_set, 104
test2
rpki::resource_set, 104
text
rpki::xml_utils::sax_handler, 687
text_attribute
rpki::left_right::list_published_-objects_elt, 329
rpki::left_right::report_error_elt, 350
rpki::publication::report_error_elt, 447
rpki::xml_utils::text_elt, 689
textwrap::TextWrapper, 690
thisUpdate
rpki::manifest::Manifest, 373
threshold
rpki::async::gc_summary, 184
timeout
rpki::https::http_client, 272
rpki::https::http_server, 294
timer
rpki::async::gc_summary, 184
rpki::https::http_stream, 302
tls
rpki::https::http_client, 272
rpki::https::http_server, 294
rpki::https::http_stream, 303
tls_accept
rpki::https::http_server, 292
tls_connect
rpki::https::http_client, 270
to_bytes
rpki::ipaddrs::v4addr, 304
rpki::ipaddrs::v6addr, 307
to_DER
rpki::x509::PEM_converter, 642
to_PEM
rpki::x509::PEM_converter, 642
to_resource_bag
rpki::up_down::class_elt, 582
to_resource_range

rpki::resource_set::roa_prefix, 484
to_resource_set
rpki::resource_set::roa_prefix_set, 491
to_rfc3779_tuple
rpki::resource_set::resource_range_-as, 459
rpki::resource_set::resource_range_-ip, 462
rpki::resource_set::resource_set_as, 473
rpki::resource_set::resource_set_ip, 476
to_roa_tuple
rpki::resource_set::roa_prefix, 484
rpki::resource_set::roa_prefix_set, 492
to_sql
rpki::sundial::datetime, 566
rpki::x509::DER_object, 639
toASN1tuple
rpki::sundial::datetime, 567
toGeneralizedTime
rpki::sundial::datetime, 567
top_opts
irbe_cli, 61
totimestamp
rpki::sundial::datetime, 567
touch_file
rpki::myrpki::CA, 377
toUTCTime
rpki::sundial::datetime, 567
toXML
rpki::left_right::list_resources_elt, 334
rpki::publication::publication_-object_elt, 442
rpki::up_down::certificate_elt, 578
rpki::up_down::class_elt, 582
rpki::up_down::class_response_-syntax, 585
rpki::up_down::error_response_pdu, 591
rpki::up_down::issue_pdu, 595
rpki::up_down::list_pdu, 600
rpki::up_down::message_pdu, 605
rpki::up_down::revoke_syntax, 615
rpki::xml_utils::base_elt, 674
rpki::xml_utils::data_elt, 680
rpki::xml_utils::msg, 683
rpki::xml_utils::text_elt, 689
toXMLtime
rpki::sundial::datetime, 567
trace
rpki::async::timer, 196
rpki::log, 92
traceback
rpki::log, 92
type
rpki::up_down::message_pdu, 606
rpki::xml_utils::msg, 683
type2name
rootd::message_pdu, 179
rpki::up_down::message_pdu, 606

u
irdbd, 66
undersized
rpki::resource_set::resource_bag, 454
unimplemented_control
rpki::xml_utils::data_elt, 680
union
rpki::resource_set::resource_bag, 455
rpki::resource_set::resource_set, 471
unwind_stack
rpki::async::iterator, 188
unwrap
rpki::x509::XML_CMS_object, 669
up_down
rpki::relaxng, 101
up_down.py(3162), 708
up_down_handler
rootd, 71
rpki::rpki_engine::rpkid_context, 544
up_down_url_regexp
rpki::rpki_engine::rpkid_context, 546
update

rpki::rpki_engine::ca_detail_obj, 510
rpki::rpki_engine::roa_obj, 537
rpki::sql::template, 562
update_children
rpki::left_right::self_elt, 363
update_roas
rpki::left_right::self_elt, 364
update_timeout
rpki::https::http_stream, 301
uri
rpki::rpki_engine::child_cert_obj, 523
rpki::rpki_engine::roa_obj, 537
uri_tail
rpki::rpki_engine::child_cert_obj, 524
rpki::rpki_engine::roa_obj, 537
uri_to_filename
rpki::publication::publication_-object_elt, 442
uris
rpki::rpki_engine::publication_-queue, 528
url
rpki::https::caller, 266
usage
irbe_cli, 60
irbe_cli::cmd_elt_mixin, 128
irbe_cli::cmd_msg_mixin, 131
usage_fill
irbe_cli, 62
use_hsm
rpki::left_right::self_elt, 366
use_internal_cron
rpki::rpki_engine::rpkid_context, 546
use_syslog
rpki::log, 93
username
rpki::sql::session, 551

v4
rpki::myrpki::child, 383
rpki::myrpki::roa_request, 412
rpki::resource_set::resource_bag, 455
v4re
rpki::myrpki::child, 383
rpki::myrpki::roa_request, 412
v6
rpki::myrpki::child, 383
rpki::myrpki::roa_request, 412
rpki::resource_set::resource_bag, 455
v6re
rpki::myrpki::child, 384
rpki::myrpki::roa_request, 412
valid_until
rpki::left_right::list_resources_elt, 335
rpki::resource_set::resource_bag, 455
validity
rpki::myrpki::child, 384
verbose
irbe_cli, 62
verify
rpki::x509::CMS_object, 622
version
rpki::https::http_message, 279
rpki::left_right::msg, 340
rpki::left_right::sax_handler, 357
rpki::manifest::Manifest, 373
rpki::myrpki, 98
rpki::publication::msg, 436
rpki::publication::sax_handler, 451
rpki::roa::RouteOriginAttestation, 503
rpki::up_down::message_pdu, 607
rpki::up_down::sax_handler, 618
rpki::xml_utils::msg, 683

want_persistent_client
rpki::https, 87
want_persistent_server
rpki::https, 87
warn
rpki::log, 93
when
rpki::async::timer, 197

whine
rpki::myrpki, 98
wired_in_config_id
rpki::publication::config_elt, 427
withdraw
rpki::rpki_engine::publication_-
queue, 528
wrap
rpki::x509::XML_CMS_object, 669
writeable
rpki::https::http_stream, 301

x509.py(3107), 708
xcert
rpki::myrpki::CA, 378
xml
rpki::myrpki::child, 382
rpki::myrpki::children, 386
rpki::myrpki::parent, 401
rpki::myrpki::parents, 404
rpki::myrpki::repositories, 406
rpki::myrpki::repository, 408
rpki::myrpki::roa_request, 411
rpki::myrpki::roa_requests, 414
xml::sax::handler::ContentHandler, 691
xml_utils.py(2836), 709
xmlns
rpki::left_right::left_right_-
namespace, 325
rpki::publication::publication_-
namespace, 438
rpki::up_down, 110

years_to_seconds
rpki::sundial::timedelta, 573
yes_or_no
rpki::cli, 79