

RPKI Engine

1.0

Generated by Doxygen 1.6.3

Tue Apr 13 21:06:48 2010

Contents

1 RPKI Engine Reference Manual	1
2 Further Reading	1
3 Installation Guide	2
4 Operation Guide	4
4.1 Common Options	6
4.2 rpkid.py	7
4.3 pubd.py	8
4.4 rootd.py	9
4.5 irdbd.py	10
4.6 irbe_cli.py	11
4.7 cross_certify.py	14
4.8 cronjob.py	14
4.9 testbed.py:	15
4.10 testpoke.py	17
5 Left-right protocol	18
5.1 Terminology	18
5.2 initiated by the IRBE	18
5.2.1 <self/> object	19
5.2.2 <bsc/> object	21
5.2.3 <parent/> object	22
5.2.4 <child/> object	23
5.2.5 <repository/> object	24
5.2.6 <route_origin/> object	25
5.3 Operations initiated by the RPKI engine	26
5.3.1 <list_resources/> messages	26
5.4 Error handling	27
6 Publication protocol	28

6.1	Terminology	28
6.2	Publication control subprotocol	28
6.2.1	<config/> object	28
6.2.2	<client/> object	29
6.3	Publication subprotocol	29
6.3.1	<certificate/> object	30
6.3.2	<crl/> object	30
6.3.3	<manifest/> object	30
6.3.4	<roa/> object	30
6.4	Error handling	30
6.5	Additional access control considerations.	31
7	SQL database schemas	32
7.1	rpkid SQL schema	34
7.2	pubd SQL Schema	39
7.3	irdbd SQL Schema	40
8	BPKI model	42
9	Namespace Documentation	45
9.1	Package irbe_cli	45
9.1.1	Detailed Description	46
9.1.2	Function Documentation	47
9.1.3	Variable Documentation	47
9.2	Package irdbd	49
9.2.1	Detailed Description	50
9.2.2	Function Documentation	50
9.2.3	Variable Documentation	51
9.3	Package pubd	53
9.3.1	Detailed Description	54
9.3.2	Function Documentation	54
9.3.3	Variable Documentation	55

9.4	Package rootd	55
9.4.1	Detailed Description	56
9.4.2	Function Documentation	57
9.4.3	Variable Documentation	59
9.5	Package rpki	63
9.6	Package rpki.__doc__	63
9.7	Package rpki.async	63
9.7.1	Detailed Description	64
9.7.2	Function Documentation	64
9.7.3	Variable Documentation	65
9.8	Package rpki.cli	66
9.8.1	Detailed Description	66
9.8.2	Function Documentation	66
9.8.3	Variable Documentation	67
9.9	Package rpki.config	67
9.9.1	Detailed Description	67
9.10	Package rpki.exceptions	68
9.10.1	Detailed Description	69
9.11	Package rpki.https	70
9.11.1	Detailed Description	71
9.11.2	Function Documentation	72
9.11.3	Variable Documentation	73
9.12	Package rpki.ipaddrs	75
9.12.1	Detailed Description	75
9.13	Package rpki.left_right	76
9.13.1	Detailed Description	76
9.13.2	Variable Documentation	77
9.14	Package rpki.log	77
9.14.1	Detailed Description	78
9.14.2	Function Documentation	78
9.14.3	Variable Documentation	79

9.15 Package rpki.manifest	80
9.15.1 Detailed Description	81
9.16 Package rpki.oids	81
9.16.1 Detailed Description	81
9.16.2 Variable Documentation	82
9.17 Package rpki.publication	83
9.17.1 Detailed Description	83
9.18 Package rpki.relaxng	84
9.18.1 Variable Documentation	84
9.19 Package rpki.resource_set	84
9.19.1 Detailed Description	85
9.19.2 Function Documentation	86
9.19.3 Variable Documentation	87
9.20 Package rpki.roa	87
9.20.1 Detailed Description	87
9.21 Package rpki.rpki_engine	88
9.21.1 Detailed Description	89
9.22 Package rpki.sql	89
9.22.1 Detailed Description	89
9.23 Package rpki.sundial	90
9.23.1 Detailed Description	90
9.23.2 Function Documentation	91
9.24 Package rpki.up_down	92
9.24.1 Detailed Description	92
9.24.2 Variable Documentation	93
9.25 Package rpki.x509	93
9.25.1 Detailed Description	94
9.25.2 Function Documentation	95
9.26 Package rpki.xml_utils	95
9.26.1 Detailed Description	96
9.27 Package rpkid	96

9.27.1 Detailed Description	96
9.27.2 Function Documentation	97
9.27.3 Variable Documentation	97
10 Class Documentation	98
10.1 <code>async_chat</code> Class Reference	98
10.2 <code>dispatcher</code> Class Reference	98
10.3 <code>Cmd</code> Class Reference	98
10.4 <code>Exception</code> Class Reference	98
10.5 <code>irbe_cli.bsc_elt</code> Class Reference	98
10.5.1 Detailed Description	100
10.5.2 Member Function Documentation	100
10.5.3 Member Data Documentation	101
10.6 <code>irbe_cli.certificate_elt</code> Class Reference	101
10.6.1 Detailed Description	102
10.7 <code>irbe_cli.child_elt</code> Class Reference	103
10.7.1 Detailed Description	105
10.8 <code>irbe_cli.client_elt</code> Class Reference	105
10.8.1 Detailed Description	107
10.9 <code>irbe_cli.cmd_elt_mixin</code> Class Reference	107
10.9.1 Detailed Description	109
10.9.2 Member Function Documentation	109
10.9.3 Member Data Documentation	111
10.10 <code>irbe_cli.cmd_msg_mixin</code> Class Reference	112
10.10.1 Detailed Description	113
10.10.2 Member Function Documentation	113
10.11 <code>irbe_cli.config_elt</code> Class Reference	113
10.11.1 Detailed Description	115
10.11.2 Member Function Documentation	115
10.11.3 Member Data Documentation	115
10.12 <code>irbe_cli.crl_elt</code> Class Reference	115

10.12.1 Detailed Description	116
10.13irbe_cli.left_right_cms_msg Class Reference	117
10.13.1 Detailed Description	118
10.13.2 Member Data Documentation	118
10.14irbe_cli.left_right_msg Class Reference	118
10.14.1 Detailed Description	120
10.14.2 Member Data Documentation	120
10.15irbe_cli.left_right_proto Class Reference	120
10.15.1 Detailed Description	121
10.15.2 Member Data Documentation	121
10.16irbe_cli.left_right_sax_handler Class Reference	122
10.16.1 Detailed Description	123
10.16.2 Member Data Documentation	123
10.17irbe_cli.list_published_objects_elt Class Reference	123
10.17.1 Detailed Description	125
10.17.2 Member Data Documentation	125
10.18irbe_cli.list_received_resources_elt Class Reference	125
10.18.1 Detailed Description	127
10.18.2 Member Data Documentation	127
10.19irbe_cli.manifest_elt Class Reference	127
10.19.1 Detailed Description	128
10.20irbe_cli.parent_elt Class Reference	129
10.20.1 Detailed Description	131
10.21irbe_cli.publication_cms_msg Class Reference	131
10.21.1 Detailed Description	132
10.21.2 Member Data Documentation	133
10.22irbe_cli.publication_msg Class Reference	133
10.22.1 Detailed Description	135
10.22.2 Member Data Documentation	135
10.23irbe_cli.publication_proto Class Reference	135
10.23.1 Detailed Description	136

10.23.2 Member Data Documentation	136
10.24irbe_cli.publication_sax_handler Class Reference	137
10.24.1 Detailed Description	138
10.24.2 Member Data Documentation	138
10.25irbe_cli.reply_elt_mixin Class Reference	138
10.25.1 Detailed Description	139
10.25.2 Member Function Documentation	139
10.25.3 Member Data Documentation	140
10.26irbe_cli.report_error_elt Class Reference	140
10.26.1 Detailed Description	141
10.27irbe_cli.repository_elt Class Reference	141
10.27.1 Detailed Description	143
10.28irbe_cli.roa_elt Class Reference	143
10.28.1 Detailed Description	144
10.29irbe_cli.self_elt Class Reference	145
10.29.1 Detailed Description	147
10.30irbe_cli.UsageWrapper Class Reference	147
10.30.1 Detailed Description	147
10.30.2 Member Function Documentation	148
10.31long Class Reference	148
10.32object Class Reference	148
10.33pubd.pubd_context Class Reference	148
10.33.1 Detailed Description	150
10.33.2 Member Function Documentation	150
10.33.3 Member Data Documentation	151
10.34datetime Class Reference	153
10.35timedelta Class Reference	153
10.36rootd.cms_msg Class Reference	153
10.36.1 Detailed Description	154
10.36.2 Member Data Documentation	155
10.37rootd.issue_pdu Class Reference	155

10.37.1 Detailed Description	156
10.37.2 Member Function Documentation	157
10.38rootd.list_pdu Class Reference	157
10.38.1 Detailed Description	158
10.38.2 Member Function Documentation	159
10.39rootd.message_pdu Class Reference	159
10.39.1 Detailed Description	161
10.39.2 Member Function Documentation	161
10.39.3 Member Data Documentation	161
10.40rootd.revoke_pdu Class Reference	162
10.40.1 Detailed Description	163
10.40.2 Member Function Documentation	163
10.41rootd.sax_handler Class Reference	163
10.41.1 Detailed Description	164
10.41.2 Member Data Documentation	165
10.42rpki.async.gc_summary Class Reference	165
10.42.1 Detailed Description	166
10.42.2 Member Function Documentation	166
10.42.3 Member Data Documentation	166
10.43rpki.async.iterator Class Reference	167
10.43.1 Detailed Description	168
10.43.2 Member Function Documentation	168
10.43.3 Member Data Documentation	169
10.44rpki.async.sync_wrapper Class Reference	170
10.44.1 Detailed Description	172
10.44.2 Member Function Documentation	172
10.44.3 Member Data Documentation	173
10.45rpki.async.timer Class Reference	173
10.45.1 Detailed Description	175
10.45.2 Member Function Documentation	176
10.45.3 Member Data Documentation	178

10.46rpki.cli.Cmd Class Reference	179
10.46.1 Detailed Description	181
10.46.2 Member Function Documentation	181
10.46.3 Member Data Documentation	183
10.47rpki.config.parser Class Reference	184
10.47.1 Detailed Description	186
10.47.2 Member Function Documentation	186
10.47.3 Member Data Documentation	188
10.48rpki.exceptions.BadClassNameSyntax Class Reference	189
10.48.1 Detailed Description	190
10.49rpki.exceptions.BadClientURL Class Reference	190
10.49.1 Detailed Description	191
10.50rpki.exceptions.BadContactURL Class Reference	191
10.50.1 Detailed Description	192
10.51rpki.exceptions.BadExtension Class Reference	192
10.51.1 Detailed Description	193
10.52rpki.exceptions.BadIRDBReply Class Reference	193
10.52.1 Detailed Description	194
10.53rpki.exceptions.BadIssueResponse Class Reference	194
10.53.1 Detailed Description	195
10.54rpki.exceptions.BadPKCS10 Class Reference	195
10.54.1 Detailed Description	196
10.55rpki.exceptions.BadPublicationReply Class Reference	196
10.55.1 Detailed Description	197
10.56rpki.exceptions.BadQuery Class Reference	197
10.56.1 Detailed Description	198
10.57rpki.exceptions.BadSender Class Reference	198
10.57.1 Detailed Description	199
10.58rpki.exceptions.BadStatusCode Class Reference	199
10.58.1 Detailed Description	200
10.59rpki.exceptions.BadURISyntax Class Reference	200

10.59.1 Detailed Description	201
10.60rpki.exceptions.BSCNotFound Class Reference	201
10.60.1 Detailed Description	202
10.61rpki.exceptions.BSCNotReady Class Reference	202
10.61.1 Detailed Description	203
10.62rpki.exceptions.ChildNotFound Class Reference	203
10.62.1 Detailed Description	204
10.63rpki.exceptions.ClassNameMismatch Class Reference	204
10.63.1 Detailed Description	205
10.64rpki.exceptions.ClassNameUnknown Class Reference	205
10.64.1 Detailed Description	206
10.65rpki.exceptions.ClientNotFound Class Reference	206
10.65.1 Detailed Description	207
10.66rpki.exceptions.CMSContentNotSet Class Reference	207
10.66.1 Detailed Description	208
10.67rpki.exceptions.CMSCRLNotSet Class Reference	209
10.67.1 Detailed Description	209
10.68rpki.exceptions.CMSVerificationFailed Class Reference	210
10.68.1 Detailed Description	210
10.69rpki.exceptions.DBConsistencyError Class Reference	211
10.69.1 Detailed Description	211
10.70rpki.exceptions.DEROBJECTConversionError Class Reference	212
10.70.1 Detailed Description	212
10.71rpki.exceptions.DuplicateObject Class Reference	213
10.71.1 Detailed Description	213
10.72rpki.exceptions.EmptyPEM Class Reference	214
10.72.1 Detailed Description	214
10.73rpki.exceptions.EmptyROAPrefixList Class Reference	215
10.73.1 Detailed Description	215
10.74rpki.exceptions.ForbiddenURI Class Reference	216
10.74.1 Detailed Description	216

10.75rpki.exceptions.HandleTranslationError Class Reference	217
10.75.1 Detailed Description	217
10.76rpki.exceptions.HTTPRequestFailed Class Reference	218
10.76.1 Detailed Description	218
10.77rpki.exceptions.HTTPSBadVersion Class Reference	219
10.77.1 Detailed Description	219
10.78rpki.exceptions.HTTPSClientAborted Class Reference	220
10.78.1 Detailed Description	220
10.79rpki.exceptions.HTTPSUnexpectedState Class Reference	221
10.79.1 Detailed Description	221
10.80rpki.exceptions.MissingCMSCRL Class Reference	222
10.80.1 Detailed Description	222
10.81rpki.exceptions.MissingCMSEcert Class Reference	223
10.81.1 Detailed Description	223
10.82rpki.exceptions.MultipleTLSEECert Class Reference	224
10.82.1 Detailed Description	225
10.83rpki.exceptions.MustBePrefix Class Reference	225
10.83.1 Detailed Description	226
10.84rpki.exceptions.NoActiveCA Class Reference	226
10.84.1 Detailed Description	227
10.85rpki.exceptions.NoCoveringCertForROA Class Reference	227
10.85.1 Detailed Description	228
10.86rpki.exceptions.NoObjectAtURI Class Reference	228
10.86.1 Detailed Description	229
10.87rpki.exceptions.NotACertificateChain Class Reference	229
10.87.1 Detailed Description	230
10.88rpki.exceptions.NotFound Class Reference	230
10.88.1 Detailed Description	231
10.89rpki.exceptions.NotImplementedYet Class Reference	231
10.89.1 Detailed Description	232
10.90rpki.exceptions.NotInDatabase Class Reference	232

10.90.1 Detailed Description	233
10.91rpki.exceptions.ReceivedTLSCACert Class Reference	233
10.91.1 Detailed Description	234
10.92rpki.exceptions.RPKI_Exception Class Reference	235
10.92.1 Detailed Description	236
10.93rpki.exceptions.ServerShuttingDown Class Reference	236
10.93.1 Detailed Description	237
10.94rpki.exceptions.SKIMismatch Class Reference	237
10.94.1 Detailed Description	238
10.95rpki.exceptions.SubprocessError Class Reference	238
10.95.1 Detailed Description	239
10.96rpki.exceptions.TLSValidation Error Class Reference	239
10.96.1 Detailed Description	240
10.97rpki.exceptions.UnexpectedCMSCerts Class Reference	241
10.97.1 Detailed Description	241
10.98rpki.exceptions.UnexpectedCMSCRLs Class Reference	242
10.98.1 Detailed Description	242
10.99rpki.exceptions.UnparsableCMS DER Class Reference	243
10.99.1 Detailed Description	243
10.10rpki.exceptions.UpstreamError Class Reference	244
10.100.1 Detailed Description	244
10.101rpki.exceptions.WrongEContent Type Class Reference	245
10.101.1 Detailed Description	245
10.102rpki.https.caller Class Reference	246
10.102.1 Detailed Description	247
10.102.2 Member Function Documentation	247
10.102.3 Member Data Documentation	247
10.103rpki.https.http_client Class Reference	248
10.103.1 Detailed Description	250
10.103.2 Member Function Documentation	250
10.103.3 Member Data Documentation	253

10.104 <pki.https.http_listener .="" .<="" class="" reference="" td=""><td>255</td></pki.https.http_listener>	255
10.104.1Detailed Description	256
10.104.2Member Function Documentation	256
10.104.3Member Data Documentation	257
10.105 <pki.https.http_message .="" .<="" class="" reference="" td=""><td>258</td></pki.https.http_message>	258
10.105.1Detailed Description	259
10.105.2Member Function Documentation	259
10.105.3Member Data Documentation	261
10.106 <pki.https.http_queue .="" .<="" class="" reference="" td=""><td>261</td></pki.https.http_queue>	261
10.106.1Detailed Description	263
10.106.2Member Function Documentation	263
10.106.3Member Data Documentation	264
10.107 <pki.https.http_request .="" .<="" class="" reference="" td=""><td>265</td></pki.https.http_request>	265
10.107.1Detailed Description	267
10.107.2Member Function Documentation	267
10.107.3Member Data Documentation	268
10.108 <pki.https.http_response .="" .<="" class="" reference="" td=""><td>268</td></pki.https.http_response>	268
10.108.1Detailed Description	270
10.108.2Member Function Documentation	270
10.108.3Member Data Documentation	270
10.109 <pki.https.http_server .="" .<="" class="" reference="" td=""><td>271</td></pki.https.http_server>	271
10.109.1Detailed Description	273
10.109.2Member Function Documentation	273
10.109.3Member Data Documentation	275
10.110 <pki.https.http_stream .="" .<="" class="" reference="" td=""><td>276</td></pki.https.http_stream>	276
10.110.1Detailed Description	278
10.110.2Member Function Documentation	279
10.110.3Member Data Documentation	284
10.111 <pki.ipaddrs.v4addr .="" .<="" class="" reference="" td=""><td>285</td></pki.ipaddrs.v4addr>	285
10.111.1Detailed Description	286
10.111.2Member Function Documentation	286

10.111.3Member Data Documentation	287
10.112pk.i.ipaddrs.v6addr Class Reference	287
10.112.1Detailed Description	288
10.112.2Member Function Documentation	289
10.112.3Member Data Documentation	289
10.113pk.i.left_right.bsc_elt Class Reference	290
10.113.1Detailed Description	292
10.113.2Member Function Documentation	292
10.113.3Member Data Documentation	293
10.114pk.i.left_right.child_elt Class Reference	295
10.114.1Detailed Description	297
10.114.2Member Function Documentation	297
10.114.3Member Data Documentation	299
10.115pk.i.left_right.cms_msg Class Reference	300
10.115.1Detailed Description	302
10.115.2Member Function Documentation	302
10.116pk.i.left_right.data_elt Class Reference	302
10.116.1Detailed Description	304
10.116.2Member Function Documentation	304
10.116.3Member Data Documentation	306
10.117pk.i.left_right.left_right_namespace Class Reference	306
10.117.1Detailed Description	307
10.117.2Member Function Documentation	307
10.118pk.i.left_right.list_published_objects_elt Class Reference	308
10.118.1Detailed Description	310
10.118.2Member Function Documentation	310
10.118.3Member Data Documentation	311
10.119pk.i.left_right.list_received_resources_elt Class Reference	311
10.119.1Detailed Description	313
10.119.2Member Function Documentation	313
10.119.3Member Data Documentation	313

10.126 <pki.left_right.list_resources_elt .="" .<="" class="" reference="" td=""><td>314</td></pki.left_right.list_resources_elt>	314
10.120.1Detailed Description	316
10.120.2Member Function Documentation	316
10.120.3Member Data Documentation	317
10.127 <pki.left_right.list_roa_requests_elt .="" .<="" class="" reference="" td=""><td>318</td></pki.left_right.list_roa_requests_elt>	318
10.121.1Detailed Description	319
10.121.2Member Function Documentation	319
10.121.3Member Data Documentation	319
10.128 <pki.left_right.msg .="" .<="" class="" reference="" td=""><td>320</td></pki.left_right.msg>	320
10.122.1Detailed Description	322
10.122.2Member Function Documentation	322
10.122.3Member Data Documentation	322
10.129 <pki.left_right.parent_elt .="" .<="" class="" reference="" td=""><td>323</td></pki.left_right.parent_elt>	323
10.123.1Detailed Description	325
10.123.2Member Function Documentation	325
10.123.3Member Data Documentation	327
10.124 <pki.left_right.report_error_elt .="" .<="" class="" reference="" td=""><td>329</td></pki.left_right.report_error_elt>	329
10.124.1Detailed Description	331
10.124.2Member Function Documentation	331
10.124.3Member Data Documentation	332
10.125 <pki.left_right.repository_elt .="" .<="" class="" reference="" td=""><td>333</td></pki.left_right.repository_elt>	333
10.125.1Detailed Description	335
10.125.2Member Function Documentation	335
10.125.3Member Data Documentation	336
10.126 <pki.left_right.sax_handler .="" .<="" class="" reference="" td=""><td>337</td></pki.left_right.sax_handler>	337
10.126.1Detailed Description	339
10.126.2Member Data Documentation	339
10.127 <pki.left_right.self_elt .="" .<="" class="" reference="" td=""><td>339</td></pki.left_right.self_elt>	339
10.127.1Detailed Description	342
10.127.2Member Function Documentation	342
10.127.3Member Data Documentation	346

10.128	pki.log.logger Class Reference	348
10.128.1	Detailed Description	349
10.128.2	Member Function Documentation	349
10.128.3	Member Data Documentation	349
10.129	pki.manifest.FileAndHash Class Reference	350
10.129.1	Detailed Description	350
10.129.2	Member Function Documentation	351
10.129.3	Member Data Documentation	351
10.130	pki.manifest.FilesAndHashes Class Reference	351
10.130.1	Detailed Description	352
10.130.2	Member Function Documentation	352
10.131	pki.manifest.Manifest Class Reference	353
10.131.1	Detailed Description	354
10.131.2	Member Function Documentation	354
10.131.3	Member Data Documentation	354
10.132	pki.publication.certificate_elt Class Reference	355
10.132.1	Detailed Description	357
10.132.2	Member Data Documentation	357
10.133	pki.publication.client_elt Class Reference	357
10.133.1	Detailed Description	359
10.133.2	Member Function Documentation	359
10.133.3	Member Data Documentation	360
10.134	pki.publication.cms_msg Class Reference	362
10.134.1	Detailed Description	364
10.134.2	Member Data Documentation	364
10.135	pki.publication.config_elt Class Reference	364
10.135.1	Detailed Description	366
10.135.2	Member Function Documentation	366
10.135.3	Member Data Documentation	367
10.136	pki.publication.control_elt Class Reference	368
10.136.1	Detailed Description	371

10.136.2Member Function Documentation	371
10.137pki.publication.crl_elt Class Reference	371
10.137.1Detailed Description	373
10.137.2Member Data Documentation	373
10.138pki.publication.manifest_elt Class Reference	373
10.138.1Detailed Description	375
10.138.2Member Data Documentation	375
10.139pki.publication.msg Class Reference	375
10.139.1Detailed Description	377
10.139.2Member Function Documentation	377
10.139.3Member Data Documentation	377
10.140pki.publication.publication_namespace Class Reference	378
10.140.1Detailed Description	378
10.140.2Member Data Documentation	379
10.141pki.publication.publication_object_elt Class Reference	379
10.141.1Detailed Description	381
10.141.2Member Function Documentation	381
10.141.3Member Data Documentation	383
10.142pki.publication.report_error_elt Class Reference	384
10.142.1Detailed Description	386
10.142.2Member Function Documentation	386
10.142.3Member Data Documentation	387
10.143pki.publication.roa_elt Class Reference	388
10.143.1Detailed Description	390
10.143.2Member Data Documentation	390
10.144pki.publication.sax_handler Class Reference	390
10.144.1Detailed Description	392
10.144.2Member Data Documentation	392
10.145pki.resource_set.resource_bag Class Reference	392
10.145.1Detailed Description	394
10.145.2Member Function Documentation	394

10.145.3Member Data Documentation	396
10.146pki.resource_set.resource_range Class Reference	397
10.146.1Detailed Description	398
10.146.2Member Function Documentation	398
10.146.3Member Data Documentation	398
10.147pki.resource_set.resource_range_as Class Reference	399
10.147.1Detailed Description	400
10.147.2Member Function Documentation	400
10.147.3Member Data Documentation	400
10.148pki.resource_set.resource_range_ip Class Reference	401
10.148.1Detailed Description	403
10.148.2Member Function Documentation	403
10.149pki.resource_set.resource_range_ipv4 Class Reference	404
10.149.1Detailed Description	406
10.149.2Member Data Documentation	406
10.150pki.resource_set.resource_range_ipv6 Class Reference	406
10.150.1Detailed Description	408
10.150.2Member Data Documentation	408
10.151pki.resource_set.resource_set Class Reference	408
10.151.1Detailed Description	410
10.151.2Member Function Documentation	410
10.151.3Member Data Documentation	412
10.152pki.resource_set.resource_set_as Class Reference	413
10.152.1Detailed Description	414
10.152.2Member Function Documentation	414
10.152.3Member Data Documentation	415
10.153pki.resource_set.resource_set_ip Class Reference	415
10.153.1Detailed Description	417
10.153.2Member Function Documentation	417
10.153.3Member Data Documentation	418
10.154pki.resource_set.resource_set_ipv4 Class Reference	418

10.154.1Detailed Description	420
10.154.2Member Data Documentation	420
10.155pkি.resource_set.resource_set_ipv6 Class Reference	420
10.155.1Detailed Description	422
10.155.2Member Data Documentation	422
10.156pkি.resource_set.roa_prefix Class Reference	422
10.156.1Detailed Description	424
10.156.2Member Function Documentation	424
10.156.3Member Data Documentation	425
10.157pkি.resource_set.roa_prefix_ipv4 Class Reference	426
10.157.1Detailed Description	428
10.157.2Member Data Documentation	428
10.158pkি.resource_set.roa_prefix_ipv6 Class Reference	428
10.158.1Detailed Description	430
10.158.2Member Data Documentation	430
10.159pkি.resource_set.roa_prefix_set Class Reference	430
10.159.1Detailed Description	431
10.159.2Member Function Documentation	432
10.160pkি.resource_set.roa_prefix_set_ipv4 Class Reference	433
10.160.1Detailed Description	435
10.160.2Member Data Documentation	435
10.161pkি.resource_set.roa_prefix_set_ipv6 Class Reference	435
10.161.1Detailed Description	437
10.161.2Member Data Documentation	437
10.162pkি.roa.ROAIPAddress Class Reference	437
10.162.1Detailed Description	438
10.162.2Member Function Documentation	438
10.162.3Member Data Documentation	439
10.163pkি.roa.ROAIPAddresses Class Reference	439
10.163.1Detailed Description	440
10.163.2Member Function Documentation	440

10.164 <pki.roa.roaipaddressfamilies .="" .<="" class="" reference="" td=""><td>440</td></pki.roa.roaipaddressfamilies>	440
10.164.1Detailed Description	441
10.164.2Member Function Documentation	441
10.165 <pki.roa.roaipaddressfamily .="" .<="" class="" reference="" td=""><td>441</td></pki.roa.roaipaddressfamily>	441
10.165.1Detailed Description	442
10.165.2Member Function Documentation	442
10.165.3Member Data Documentation	443
10.166 <pki.roa.routeoriginattestation .="" .<="" class="" reference="" td=""><td>443</td></pki.roa.routeoriginattestation>	443
10.166.1Detailed Description	444
10.166.2Member Function Documentation	444
10.166.3Member Data Documentation	444
10.167 <pki.rpki_engine.ca_detail_obj .="" .<="" class="" reference="" td=""><td>445</td></pki.rpki_engine.ca_detail_obj>	445
10.167.1Detailed Description	447
10.167.2Member Function Documentation	448
10.167.3Member Data Documentation	452
10.168 <pki.rpki_engine.ca_obj .="" .<="" class="" reference="" td=""><td>454</td></pki.rpki_engine.ca_obj>	454
10.168.1Detailed Description	456
10.168.2Member Function Documentation	456
10.168.3Member Data Documentation	460
10.169 <pki.rpki_engine.child_cert_obj .="" .<="" class="" reference="" td=""><td>461</td></pki.rpki_engine.child_cert_obj>	461
10.169.1Detailed Description	463
10.169.2Member Function Documentation	463
10.169.3Member Data Documentation	465
10.170 <pki.rpki_engine.publication_queue .="" .<="" class="" reference="" td=""><td>466</td></pki.rpki_engine.publication_queue>	466
10.170.1Detailed Description	468
10.170.2Member Function Documentation	468
10.170.3Member Data Documentation	469
10.171 <pki.rpki_engine.revoked_cert_obj .="" .<="" class="" reference="" td=""><td>470</td></pki.rpki_engine.revoked_cert_obj>	470
10.171.1Detailed Description	471
10.171.2Member Function Documentation	471
10.171.3Member Data Documentation	472

10.172	pki.rpki_engine.roa_obj Class Reference	473
10.172.1	Detailed Description	475
10.172.2	Member Function Documentation	475
10.172.3	Member Data Documentation	478
10.173	pki.rpki_engine.rpkid_context Class Reference	480
10.173.1	Detailed Description	482
10.173.2	Member Function Documentation	483
10.173.3	Member Data Documentation	485
10.174	pki.sql.session Class Reference	488
10.174.1	Detailed Description	489
10.174.2	Member Function Documentation	490
10.174.3	Member Data Documentation	491
10.175	pki.sql.sql_persistent Class Reference	493
10.175.1	Detailed Description	495
10.175.2	Member Function Documentation	495
10.175.3	Member Data Documentation	499
10.176	pki.sql.template Class Reference	500
10.176.1	Detailed Description	502
10.176.2	Member Function Documentation	502
10.176.3	Member Data Documentation	502
10.177	pki.sundial.datetime Class Reference	503
10.177.1	Detailed Description	505
10.177.2	Member Function Documentation	505
10.177.3	Member Data Documentation	509
10.178	pki.sundial.timedelta Class Reference	509
10.178.1	Detailed Description	511
10.178.2	Member Function Documentation	512
10.178.3	Member Data Documentation	514
10.179	pki.up_down.base_elt Class Reference	515
10.179.1	Detailed Description	516
10.179.2	Member Function Documentation	516

10.180 <pki.up_down.certificate_elt .="" .<="" class="" reference="" td=""><td>517</td></pki.up_down.certificate_elt>	517
10.180.1Detailed Description	519
10.180.2Member Function Documentation	519
10.180.3Member Data Documentation	520
10.181 <pki.up_down.class_elt .="" .<="" class="" reference="" td=""><td>520</td></pki.up_down.class_elt>	520
10.181.1Detailed Description	522
10.181.2Member Function Documentation	522
10.181.3Member Data Documentation	523
10.182 <pki.up_down.class_response_syntax .="" .<="" class="" reference="" td=""><td>525</td></pki.up_down.class_response_syntax>	525
10.182.1Detailed Description	526
10.182.2Member Function Documentation	526
10.182.3Member Data Documentation	527
10.183 <pki.up_down.cms_msg .="" .<="" class="" reference="" td=""><td>527</td></pki.up_down.cms_msg>	527
10.183.1Detailed Description	529
10.183.2Member Function Documentation	529
10.184 <pki.up_down.error_response_pdu .="" .<="" class="" reference="" td=""><td>529</td></pki.up_down.error_response_pdu>	529
10.184.1Detailed Description	531
10.184.2Member Function Documentation	531
10.184.3Member Data Documentation	532
10.185 <pki.up_down.issue_pdu .="" .<="" class="" reference="" td=""><td>533</td></pki.up_down.issue_pdu>	533
10.185.1Detailed Description	535
10.185.2Member Function Documentation	535
10.185.3Member Data Documentation	536
10.186 <pki.up_down.issue_response_pdu .="" .<="" class="" reference="" td=""><td>537</td></pki.up_down.issue_response_pdu>	537
10.186.1Detailed Description	538
10.186.2Member Function Documentation	539
10.187 <pki.up_down.list_pdu .="" .<="" class="" reference="" td=""><td>539</td></pki.up_down.list_pdu>	539
10.187.1Detailed Description	541
10.187.2Member Function Documentation	541
10.188 <pki.up_down.list_response_pdu .="" .<="" class="" reference="" td=""><td>542</td></pki.up_down.list_response_pdu>	542
10.188.1Detailed Description	542

10.189	pki.up_down.message_pdu Class Reference	543
10.189.1	Detailed Description	545
10.189.2	Member Function Documentation	545
10.189.3	Member Data Documentation	547
10.190	pki.up_down.multi_uri Class Reference	548
10.190.1	Detailed Description	549
10.190.2	Member Function Documentation	549
10.191	pki.up_down.revoke_pdu Class Reference	550
10.191.1	Detailed Description	552
10.191.2	Member Function Documentation	552
10.191.3	Member Data Documentation	553
10.192	pki.up_down.revoke_response_pdu Class Reference	553
10.192.1	Detailed Description	554
10.193	pki.up_down.revoke_syntax Class Reference	555
10.193.1	Detailed Description	556
10.193.2	Member Function Documentation	556
10.193.3	Member Data Documentation	556
10.194	pki.up_down.sax_handler Class Reference	557
10.194.1	Detailed Description	559
10.194.2	Member Function Documentation	559
10.195	pki.x509.CMS_object Class Reference	559
10.195.1	Detailed Description	562
10.195.2	Member Function Documentation	562
10.195.3	Member Data Documentation	563
10.196	pki.x509.CRL Class Reference	566
10.196.1	Detailed Description	567
10.196.2	Member Function Documentation	567
10.196.3	Member Data Documentation	569
10.197	pki.x509.DeadDrop Class Reference	570
10.197.1	Detailed Description	571
10.197.2	Member Function Documentation	571

10.197.3Member Data Documentation	571
10.198pki.x509.DER_CMS_object Class Reference	572
10.198.1Detailed Description	573
10.198.2Member Function Documentation	573
10.198.3Member Data Documentation	573
10.199pki.x509.DER_object Class Reference	574
10.199.1Detailed Description	576
10.199.2Member Function Documentation	576
10.199.3Member Data Documentation	581
10.200pki.x509.PEM_converter Class Reference	582
10.200.1Detailed Description	583
10.200.2Member Function Documentation	583
10.200.3Member Data Documentation	584
10.201pki.x509.PKCS10 Class Reference	584
10.201.1Detailed Description	586
10.201.2Member Function Documentation	586
10.201.3Member Data Documentation	587
10.202pki.x509.ROA Class Reference	588
10.202.1Detailed Description	590
10.202.2Member Function Documentation	590
10.202.3Member Data Documentation	590
10.203pki.x509.RSA Class Reference	591
10.203.1Detailed Description	593
10.203.2Member Function Documentation	593
10.203.3Member Data Documentation	594
10.204pki.x509.RSAPublic Class Reference	595
10.204.1Detailed Description	597
10.204.2Member Function Documentation	597
10.204.3Member Data Documentation	598
10.205pki.x509.SignedManifest Class Reference	599
10.205.1Detailed Description	600

10.205.2Member Function Documentation	600
10.205.3Member Data Documentation	601
10.206pkix509.X509 Class Reference	601
10.206.1Detailed Description	603
10.206.2Member Function Documentation	603
10.206.3Member Data Documentation	606
10.207pkix509.XML_CMS_object Class Reference	607
10.207.1Detailed Description	609
10.207.2Member Function Documentation	609
10.207.3Member Data Documentation	611
10.208pkixml_utils.base_elt Class Reference	611
10.208.1Detailed Description	613
10.208.2Member Function Documentation	613
10.208.3Member Data Documentation	615
10.209pkixml_utils.data_elt Class Reference	616
10.209.1Detailed Description	618
10.209.2Member Function Documentation	618
10.210pkixml_utils.msg Class Reference	621
10.210.1Detailed Description	623
10.210.2Member Function Documentation	623
10.210.3Member Data Documentation	624
10.211pkixml_utils.sax_handler Class Reference	625
10.211.1Detailed Description	626
10.211.2Member Function Documentation	626
10.211.3Member Data Documentation	628
10.212pkixml_utils.text_elt Class Reference	629
10.212.1Detailed Description	630
10.212.2Member Function Documentation	630
10.212.3Member Data Documentation	630
10.21\$equence Class Reference	631
10.21\$equenceOf Class Reference	631

10.21TextWrapper Class Reference	631
10.21ContentHandler Class Reference	631
11 File Documentation	632
11.1 __doc__.py File Reference	632
11.2 __init__.py File Reference	632
11.3 async.py File Reference	632
11.4 cli.py File Reference	633
11.5 config.py File Reference	633
11.6 exceptions.py File Reference	633
11.7 https.py File Reference	635
11.8 ipaddrs.py File Reference	636
11.9 irbe_cli.py File Reference	637
11.10irdbd.py File Reference	638
11.11left_right.py File Reference	639
11.12log.py File Reference	639
11.13manifest.py File Reference	640
11.14oids.py File Reference	640
11.15pubd.py File Reference	641
11.16publication.py File Reference	641
11.17relaxng.py File Reference	642
11.18resource_set.py File Reference	642
11.19roa.py File Reference	643
11.20rootd.py File Reference	644
11.21rpki_engine.py File Reference	645
11.22rpkid.py File Reference	646
11.23sql.py File Reference	646
11.24sundial.py File Reference	646
11.25up_down.py File Reference	647
11.26x509.py File Reference	647
11.27xml_utils.py File Reference	648

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:

- The [installation instructions](#)
- The [operation instructions](#)
- 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 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](#)
- [APNIC's project Trac instance](#)

3 Installation Guide

Preliminary 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. 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/>. lxml in turn requires the Gnome LibXML2 C libraries.
 - FreeBSD: /usr/ports/devel/py-lxml
 - Fedora: python-lxml.i386
 - Ubuntu: python-lxml
- <http://sourceforge.net/projects/mysql-python/>. 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 statically 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.

You will also need a MySQL installation. This code was developed using MySQL 5.1 and has been tested with MySQL 5.0 and 5.1.

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. You will probably want to test it. All tests should be run from the rpkid/ directory. The test suite requires a few more external packages, only one of which is Python code.

- <http://pyyaml.org/>. testpoke.py (an up-down protocol command line test client) and testbed.py (a test harness) use PyYAML.
 - 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

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/testbed.setup.sql. The MySQL command line client is usually the easiest way to do this, eg:

```
$ cd $top/rpkid  
$ mysql -u root -p <testbed.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://lynx.isc.org/current/>. The documentation build process uses xsltproc and Lynx to dump flat text versions of a few critical documentation pages.
 - FreeBSD: /usr/ports/www/lynx
 - Ubuntu: lynx
- <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

4 Operation Guide

Preliminary operation instructions for rpkid et al.

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

Warning

rpkid is still in development, and the code changes more often than the hand-maintained portions of this documentation. The following text was reasonably accurate at the time it was written but may be obsolete by the time you read it.

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.py`: The main RPKI engine daemon.
- `pubd.py`: The publication engine daemon.
- `rootd.py`: 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.py`: A sample implementation of an IR database daemon. rpkid calls into this to perform lookups via the left-right protocol.
- `irbe_cli.py`: A command-line client for the left-right control protocol.
- `cross_certify.py`: A BPKI cross-certification tool.
- `cronjob.py`: A trivial HTTP client used to drive rpkid cron events.
- `testbed.py`: A test tool for running a collection of rpkid and irdb instances under common control, driven by a unified test script.
- `testpoke.py`: A simple client for the up-down protocol, mostly compatible with APNIC's `rpkid_poke.pl` tool.

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 `testbed.py` 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, starting rpkid, pubd, rootd, and irdbd, using the left-right control protocol to set up rpkid's internal state, and setting up a cron job to invoke rpkid's cron action at regular intervals. 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.

Note that the full event-driven model for rpkid hasn't yet been implemented. The design is intended to allow an arbitrary number of hosted RPKI engines to run in a single rpkid instance, but without the event-driven tasking model one must set up a separate rpkid instance for each hosted RPKI engine.

At present the daemon programs all run in foreground, that is, if one wants them to run in background one must do so manually, eg, using Bourne shell syntax:

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

All of the daemons use syslog by default. To make them log to stderr instead, use the "-d" option.

4.1 Common 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.

4.2 rpkid.py

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. In production use the latter stage would be handled by the IRBE stub; for test and development purposes it's handled by the [irbe_cli.py](#) command line interface or by the testbed.py test framework.

rpkid stores dynamic data in an SQL database, which must have been created for it, as explained in the [installation guide](#).

The 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.

4.3 pubd.py

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 rcync 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.

The default config file is pubd.conf, start pubd with "-c filename" to choose a different config file. All options are in the section "[pubd]". Certificates, 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.

- `bpkি-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/".

4.4 rootd.py

rootd is a stripped down implementation 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.

The 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:

- `bpkি-ta`: Name of file containing BPKI trust anchor. All BPKI certificate validation in rootd traces back to this trust anchor.
- `rootd-bpkি-cert`: Name of file containing rootd's own BPKI certificate.
- `rootd-bpkি-key`: Name of file containing RSA key corresponding to `rootd-bpkি-cert`.
- `rootd-bpkি-crl`: Name of file containing BPKI CRL that would cover `rootd-bpkি-cert` had it been revoked.

- `child-bpki-cert`: Name of file containing BPKI certificate for roott's one and only child (RPKI engine to which roott 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.
- `rpkি-root-key`: Name of file containing RSA key to use in signing resource certificates.
- `rpkি-root-cert`: Name of file containing self-signed root resource certificate corresponding to `rpkি-root-key`.
- `rpkি-root-dir`: Name of directory where roott should write RPKI subject certificate, manifest, and CRL.
- `rpkি-subject-cert`: Name of file that roott should use to save the one and only certificate it issues. Default is "Subroot.cer".
- `rpkি-root-crl`: Name of file to which roott should save its RPKI CRL. Default is "Root.crl".
- `rpkি-root-manifest`: Name of file to which roott should save its RPKI manifest. Default is "Root.mnf".
- `rpkি-subject-pkcs10`: Name of file that roott 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.

4.5 irdbd.py

irdbd is a sample implementation 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 IDs (foreign keys into rpkid's database, basically) in the IRDB.

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.
- **bpkı-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.
- **rpkıd-cert**: Name of file containing certificate used the one and only by rpkıd instance authorized to contact this irdbd instance.
- **https-url**: Service URL for irdbd. Must be a https:// URL.

4.6 irbe_cli.py

[irbe_cli](#) is a simple command line client for the control subsets of the [left-right](#) and [publication](#) protocols. In production use this functionality would be part of the IRBE stub.

Basic configuration of [irbe_cli](#) is handled via a config file. The specific action or actions to be performed are specified on the command line, and map closely to the protocols themselves.

At present the user is assumed to be able to read the (XML) left-right and publication protocol messages, and with one exception, irdbd-cli makes no attempt to interpret the responses other than to check for signature and syntax errors. The one exception is that, if the `--pem_out` option is specified on the command line, any PKCS #10 requests received from rpkıd will be written in PEM format to that file; this makes it easier to hand these requests off to the business PKI (BPKI in order to issue signing certs corresponding to newly generated business keys.

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

\$Id: irbe_cli.py 2799 2009-09-30 02:33:36Z 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.

Usage:

```
# Top-level options:
--config= --help --pem_out= --quiet --verbose

# left-right protocol:
parent --action= --tag= --self_handle= --parent_handle= --bsc_handle=
--repository_handle= --peer_contact_uri= --sia_base=
--sender_name= --recipient_name= --bpki_cms_cert= --bpki_cms_glue=
--bpki_https_cert= --bpki_https_glue= --rekey --reissue --revoke
--revoke_forgotten
repository --action= --tag= --self_handle= --repository_handle=
--bsc_handle= --peer_contact_uri= --bpki_cert= --bpki_glue=
self --action= --tag= --self_handle= --crl_interval= --regen_margin=
--bpki_cert= --bpki_glue= --rekey --reissue --revoke --run_now
--publish_world_now --revoke_forgotten
child --action= --tag= --self_handle= --child_handle= --bsc_handle=
--bpki_cert= --bpki_glue= --reissue
list_published_objects --self_handle= --tag=
bsc --action= --tag= --self_handle= --bsc_handle= --key_type=
--hash_alg= --key_length= --signing_cert= --signing_cert_crl=
--generate_keypair

# publication protocol:
certificate --action= --tag= --client_handle= --uri=
```

```

roa --action= --tag= --client_handle= --uri=
manifest --action= --tag= --client_handle= --uri=
client --action= --tag= --client_handle= --base_uri= --bpki_cert=
--bpki_glue=
config --action= --tag= --bpki_crl=
crl --action= --tag= --client_handle= --uri=

```

Global options (`--config`, `--help`, `--pem_out`) come first, then zero or more commands (`parent`, `repository`, `self`, `child`, `bsc`, `config`, `client`), each followed by its own set of options. The commands map to elements in the protocols, and the command-specific options map to attributes or subelements for those commands.

`--tag` is an optional arbitrary tag (think IMAP) to simplify matching up replies with batched queries.

`--*_handle` options refer to object primary keys.

The remaining options are specific to the particular commands, and follow directly from the protocol specifications.

A trailing "`=`" in the above option summary indicates that an option takes a value, eg, "`--action create`" or "`--action=create`". Options without a trailing "`=`" correspond to boolean control attributes.

The default config file for `irbe_cli` is `irbe_cli.conf`, start `irbe_cli` with "`-c filename`" (or "`--config filename`") to choose a different config file. All options are in the section "[`irbe_cli`]". Certificates, keys, and trust anchors may be in either DER or PEM format.

Config file options:

- `rpkid-bpki-ta`: Name of file containing BPKI trust anchor to use when authenticating messages from rpkid.
- `rpkid-irbe-cert`: Name of file containing BPKI certificate `irbe_cli` should use when talking to rpkid.
- `rpkid-irbe-key`: Name of file containing RSA key corresponding to `rpkid-irbe-cert`.
- `rpkid-cert`: Name of file containing rpkid's BPKI certificate.
- `rpkid-url`: Service URL for rpkid. Must be a https:// URL.
- `pubd-bpki-ta`: Name of file containing BPKI trust anchor to use when authenticating messages from pubd.
- `pubd-irbe-cert`: Name of file containing BPKI certificate `irbe_cli` should use when talking to pubd.

- pubd-irbe-key: Name of file containing RSA key corresponding to pubd-irbe-cert.
- pubd-cert: Name of file containing pubd's BPKI certificate.
- pubd-url: Service URL for pubd. Must be a https:// URL.

4.7 cross_certify.py

cross_certify.py is a small tool to extract certain fields from an existing X.509 certificate and generate issue a new certificate that can be used as part of a cross-certification chain. cross_certify doesn't take a config file, all of its arguments are specified on the command line.

```
python cross_certify.py { -i | --in      } input_cert
                        { -c | --ca      } issuing_cert
                        { -k | --key     } issuing_cert_key
                        { -s | --serial  } serial_filename
                        [ { -h | --help  } ]
                        [ { -o | --out   }     filename ]
                        [ { -l | --lifetime } timedelta ]
```

4.8 cronjob.py

This is a trivial program to trigger a cron run within rpkid. Ordinarily rpkid runs its own internal cron process, but for scripted testing it is sometimes useful to be able to control when cron cycles occur.

The default config file is cronjob.conf, start cronjob with "-c filename" to choose a different config file. All options are in the section "[cronjob]". 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.
- irbe-cert: Name of file containing cronjob.py's BPKI certificate.
- https-key: Name of file containing RSA key corresponding to irbe-cert.
- rpkid-cert: Name of file containing rpkid's BPKI certificate.
- https-url: Service URL for rpkid. Must be a https:// URL.

4.9 testbed.py:

testbed is a test harness to set up and run a collection of rpkid and irdbd instances under scripted control. testbed is a very recent addition to the toolset and is still evolving rapidly.

Unlike the programs described above, testbed 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. testbed 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.

All of the options in the first (optional) configuration file are just overrides for wired-in default values. In most cases the defaults will suffice, and the set of options is still in flux, so only a few of the options are described here. The default name for this configuration file is testbed.conf, run testbed with "-c filename" to change it.

testbed.conf options:

- `testbed_dir`: Working directory into which testbed should write the (many) files it generates. Default is "testbed.dir".
- `irdb_db_pass`: MySQL password for the "irdb" user. Default is "fnord". You may want to override this.
- `rpk_i_db_pass`: MySQL password for the "rpk_i" user. Default is "fnord". You may want to override this.
- `rootd_sia`: rsync URI naming a (perhaps fictitious) directory to use as the id-ad-caRepository SIA value in the generated root resource certificate. Default is "rsync://wombat.invalid/". You may want to override this if you intend to run an rsync server and test against the generated results using rcynic. This default will likely change if and when testbed learns how to run rcynic itself as part of the test suite.

The second configuration file is named testbed.yaml by default, run testbed 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". The details are still evolving, but here's an example of current usage:

```

name:          RIR
valid_for:    2d
sia_base:     "rsync://wombat.invalid/"
kids:
  - name: LIRO
  kids:
    - name: Alice
      ipv4: 192.0.2.1-192.0.2.33
      asn: 64533
    ---
    - name: Alice
      valid_add: 10
    ---
    - name: Alice
      add_as: 33
      valid_add: 2d
    ---
    - name: Alice
      valid_sub: 2d
    ---
    - name: Alice
      valid_for: 10d
  
```

This specifies an initial layout consisting of an RPKI engine named "RIR", with one child "LIRO", which in turn has one child "Alice". Alice 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 Alice's resources and makes no other modifications. The second subsequent document grants Alice additional resources and adds another two days to the validity interval for Alice's resources. The next document subtracts two days from the validity interval for Alice's resources. The final document sets the validity interval for Alice's resources to ten days.

Operators in subsequent (update) documents:

- `add_as, add_v4, add_v6`: These add ASN, IPv4, or IPv6 resources, respectively.
- `sub_as, sub_v4, sub_v6`: These subtract resources.
- `valid_until`: Set an absolute expiration date.
- `valid_for`: Set a relative expiration date.
- `valid_add, valid_sub`: Add to or subtract from validity interval.
- `sleep [interval]`: Sleep for specified interval, or until testbed receives a SIGALRM signal.

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".

4.10 testpoke.py

This is a command-line client for the up-down protocol. Unlike all of the above programs, testpoke does not accept a config file in OpenSSL-compatable format at all. Instead, it is configured exclusively by a YAML script. testpoke's design was constrained by a desire to have it be compatable with APNIC's rpki_poke.pl tool, so that the two tools could use a common configuration language to simplify scripted testing. There are minor variations due to slightly different feature sets, but YAML files intended for one program will usually work with the other.

README for APNIC's tool describing the input language can be found at <http://mirin.apnic.net/svn/rpki-engine/branches/gary-poker/client/poke/README>.

testpoke.py takes a simplified command line and uses only one YAML input file.

```
Usage: python testpoke.py [ { -y | --yaml } configfile ]
                           [ { -r | --request } requestname ]
                           [ { -h | --help } ]
```

Default configuration file is testpoke.yaml, override with --yaml option.

The --request option specifies the specific command within the YAML file to execute.

Sample configuration file:

```
---
# Sample YAML configuration file for testpoke.py

version: 1
posturl: https://localhost:4433/up-down/1
recipient-id: wombat
sender-id: "1"

cms-cert-file: biz-certs/Frank-EE.cer
cms-key-file: biz-certs/Frank-EE.key
cms-ca-cert-file: biz-certs/Bob-Root.cer
cms-cert-chain-file: [ biz-certs/Frank-CA.cer ]

ssl-cert-file: biz-certs/Frank-EE.cer
ssl-key-file: biz-certs/Frank-EE.key
```

```

ssl-ca-cert-file: biz-certs/Bob-Root.cer

requests:
  list:
    type: list
    issue:
      type: issue
      class: 1
      sia: [ "rsync://bandicoot.invalid/some/where/" ]
      revoke:
        type: revoke
        class: 1
      ski: "CB5K6APY-4KcGAW9jaK_cVPXKX0"

```

testpoke adds one extension to the language described in APNIC's README: the `cms-cert-chain-*` and `ssl-cert-chain-*` options, which allow one to specify a chain of intermediate certificates to be presented in the CMS or TLS protocol. APNIC's initial implementation required direct knowledge of the issuing certificate (ie, it supported a maximum chain length of one); subsequent APNIC code changes have probably relaxed this restriction, and with luck APNIC has copied testpoke's syntax to express chains of intermediate certificates.

5 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.

5.1 Terminology

- *IRBE*: Internet Registry Back End
- *IRDB*: Internet Registry Data Base
- *BPKI*: Business PKI
- *RPKI*: Resource PKI

5.2 initiated by the IRBE

This part of the protocol 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.

5.2.1 <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 certificate 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 propagate 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.

5.2.2 `<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.

5.2.3 <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.

5.2.4 <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.

5.2.5 <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.

5.2.6 <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".

5.3 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.

5.3.1 <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.

5.4 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 capability is not used, debugging information goes to syslog.

6 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.

6.1 Terminology

- *IRBE*: Internet Registry Back End
- *IRDB*: Internet Registry Data Base
- *BPKI*: Business PKI
- *RPKI*: Resource PKI

6.2 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.

6.2.1 <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:

- `bpk_i_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.

6.2.2 <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.
- `bpk_i_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 `bpk_i_glue` certificate is in use (below), the `bpk_i_cert` certificate should be issued by the `bpk_i_glue` certificate; otherwise, the `bpk_i_cert` certificate should be issued by the publication engine's `bpk_i_ta` certificate.
- `bpk_i_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 `bpk_i_glue` certificate should be the issuer of the `bpk_i_cert` certificate and should be issued by the publication engine's `bpk_i_ta` certificate; if not needed, the `bpk_i_glue` certificate should be left unset.

6.3 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 the 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.

6.3.1 <certificate/> object

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

6.3.2 <crl/> object

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

6.3.3 <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.

6.3.4 <roa/> object

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

6.4 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 capability is not used, debugging information goes to syslog.

6.5 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,

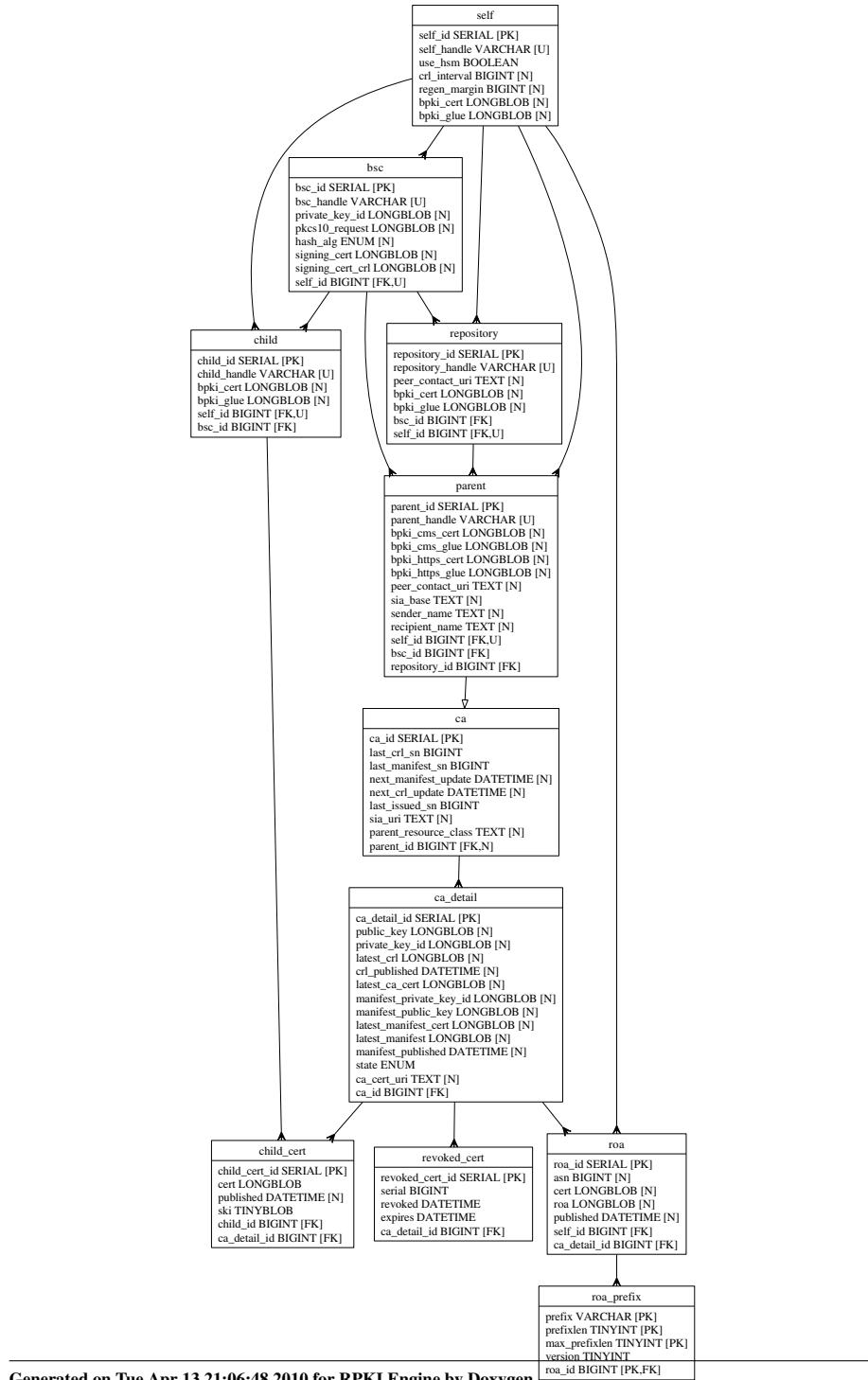
using the current published data before withdrawing it. The latter in turn implies an ordering constraint on "withdraw" actions in order to preserve the data necessary for these access control decisions; as this may prove impractical, the publication server may probably need to make periodic sweeps over 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.

7 SQL database schemas

- [rpkid database schema](#)
- [pubd database schema](#)
- [irdbd database schema](#)

7.1 rpkid SQL schema



Generated on Tue Apr 13 21:06:48 2010 for RPKI Engine by Doxygen

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
                      (self_id) REFERENCES self (self_id) ON DELETE CASCADE,
    FOREIGN KEY      (self_id, bsc_handle)
    UNIQUE
) 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
                      (self_id) REFERENCES self (self_id) ON DELETE CASCADE,
    FOREIGN KEY      (repository_id, bsc_id)
    CONSTRAINT        repository_bsc_id
                      (bsc_id) REFERENCES bsc (bsc_id) ON DELETE CASCADE,
    UNIQUE
) 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
                      (repository_id) REFERENCES repository (repository_id) ON DELETE CASCADE,
    FOREIGN KEY        (repository_id, bsc_id)
    CONSTRAINT         parent_bsc_id
                      (bsc_id) REFERENCES bsc (bsc_id) ON DELETE CASCADE,
    CONSTRAINT         parent_self_id
                      (self_id) REFERENCES self (self_id) ON DELETE CASCADE,
    UNIQUE
) 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 parent 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)
) ENGINE=InnoDB;

```

```
PRIMARY KEY  
CONSTRAINT  
FOREIGN KEY  
CONSTRAINT  
FOREIGN KEY  
) ENGINE=InnoDB;  
  
CREATE TABLE revoked_cert (  
    revoked_cert_id  
    serial  
    revoked  
    expires  
    ca_detail_id  
    PRIMARY KEY  
    CONSTRAINT  
    FOREIGN KEY  
) ENGINE=InnoDB;  
  
CREATE TABLE roa (  
    roa_id  
    asn  
    cert  
    roa  
    published  
    self_id  
    ca_detail_id  
    PRIMARY KEY  
    CONSTRAINT  
    FOREIGN KEY  
    CONSTRAINT  
    FOREIGN KEY  
) ENGINE=InnoDB;  
  
CREATE TABLE roa_prefix (   
    prefix  
    prefixlen  
    max_prefixlen  
    version  
    roa_id  
    PRIMARY KEY  
    CONSTRAINT  
    FOREIGN KEY  
) ENGINE=InnoDB;  
  
-- Local Variables:  
-- indent-tabs-mode: nil  
-- End:
```

7.2 pubd SQL Schema

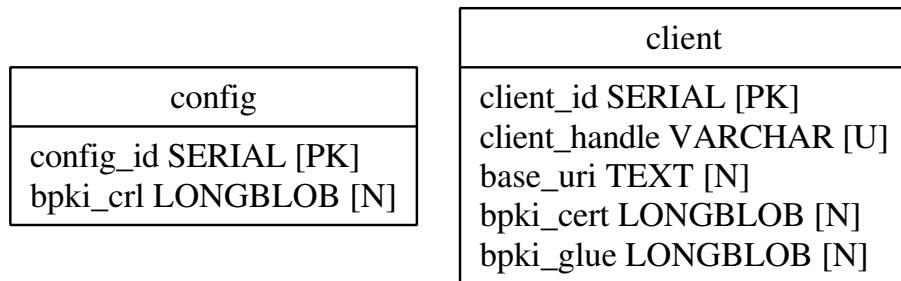


Figure 2: Diagram of pubd.sql

```

-- $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,
    bpk_i_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,
    bpk_i_cert     LONGBLOB,
    bpk_i_glue    LONGBLOB,
    PRIMARY KEY    (client_id),
    UNIQUE         (client_handle)
) ENGINE=InnoDB;

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

```

7.3 irdbd SQL Schema

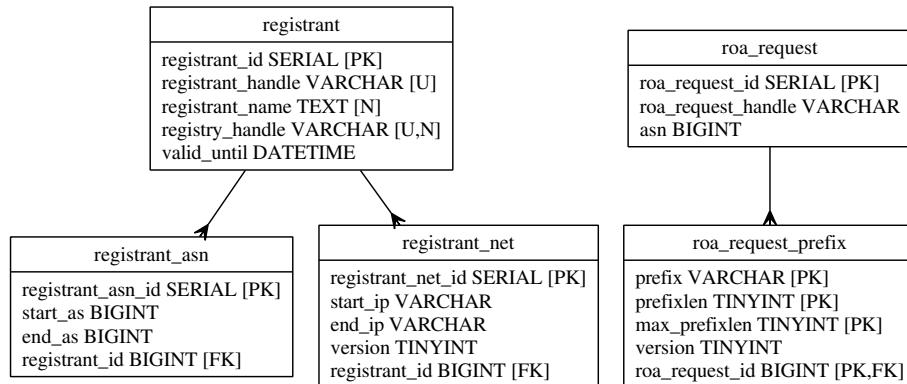


Figure 3: Diagram of irdbd.sql

```

-- $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 CASCADE
) 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 CASCADE
) 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 CASCADE
) ENGINE=InnoDB;

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

```

8 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 name "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.

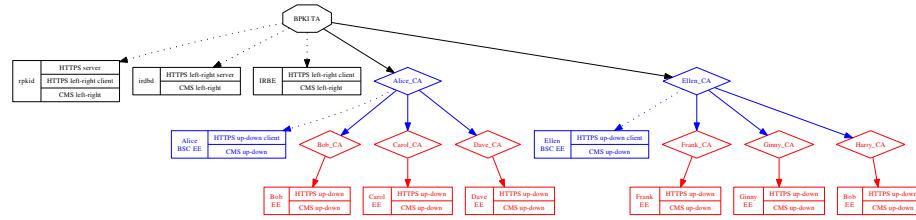
There are a few design principals that underly the chosen BPKI model:

- 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.

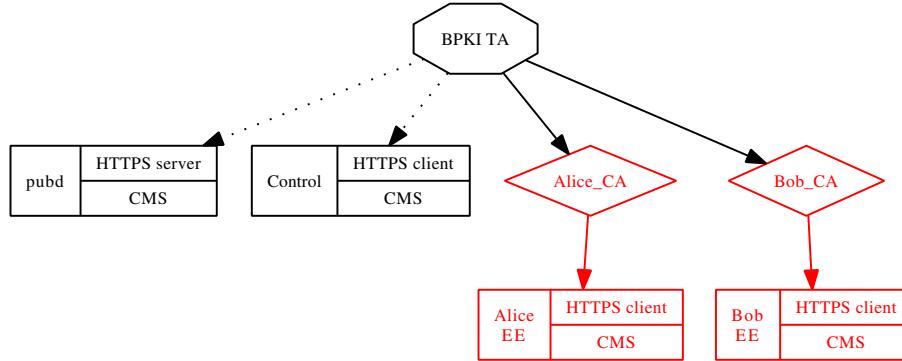
The certificate tree looks complicated, but the set of certificates needed to build any particular validation chain is obvious, again excepting the HTTPS server case, where the client certificate is the first hint that the engine has of the client's identity, so the server must be prepared to accept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

9 Namespace Documentation

9.1 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

9.1.1 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.

9.1.2 Function Documentation

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

Definition at line 240 of file irbe_cli.py.

9.1.3 Variable Documentation

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

Definition at line 259 of file irbe_cli.py.

9.1.3.2 tuple irbe_cli.call_pubd

Initial value:

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

Definition at line 323 of file irbe_cli.py.

9.1.3.3 tuple irbe_cli.call_rpkid

Initial value:

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

Definition at line 306 of file irbe_cli.py.

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

Definition at line 283 of file irbe_cli.py.

9.1.3.5 irbe_cli.cfg_file = "irbe.conf"

Definition at line 264 of file irbe_cli.py.

9.1.3.6 irbe_cli.pem_out = None

Definition at line 39 of file irbe_cli.py.

9.1.3.7 irbe_cli.q_msg = q_msg_left_right

Definition at line 291 of file irbe_cli.py.

9.1.3.8 list irbe_cli.q_msg_left_right = []

Definition at line 285 of file irbe_cli.py.

9.1.3.9 list irbe_cli.q_msg_publication = []

Definition at line 286 of file irbe_cli.py.

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

Definition at line 290 of file irbe_cli.py.

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

Definition at line 238 of file irbe_cli.py.

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

Definition at line 50 of file irbe_cli.py.

9.1.3.13 irbe_cli.verbose = True

Definition at line 265 of file irbe_cli.py.

9.2 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"))

9.2.1 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.

9.2.2 Function Documentation

9.2.2.1 def `irdbd.handle_list_resources (q_pdu, r_msg)`

Definition at line 53 of file `irdbd.py`.

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

Definition at line 90 of file irdbd.py.

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

Definition at line 119 of file irdbd.py.

9.2.3 Variable Documentation**9.2.3.1 tuple irdbd.bpkita = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))**

Definition at line 201 of file irdbd.py.

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

Definition at line 186 of file irdbd.py.

9.2.3.3 irdbd.cfg_file = "irdbd.conf"

Definition at line 170 of file irdbd.py.

9.2.3.4 tuple irdbd.client_ta = (bpki_ta, rpkid_cert)

Definition at line 217 of file irdbd.py.

9.2.3.5 tuple irdbd.cur = db.cursor()

Definition at line 198 of file irdbd.py.

9.2.3.6 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.

9.2.3.7 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.

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

Definition at line 220 of file irdbd.py.

9.2.3.9 string irdbd.host = "localhost"

Definition at line 218 of file irdbd.py.

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

Definition at line 203 of file irdbd.py.

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

Definition at line 204 of file irdbd.py.

9.2.3.12 int irdbd.port = 443

Definition at line 219 of file irdbd.py.

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

Definition at line 202 of file irdbd.py.

9.2.3.14 irdbd.server_cert = irdbd_cert,

Definition at line 216 of file irdbd.py.

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

Definition at line 188 of file irdbd.py.

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

Definition at line 206 of file irdbd.py.

9.3 Package pubd

Classes

- class [pubd_context](#)

Functions

- def [main](#)

Variables

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

9.3.1 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.

9.3.2 Function Documentation

9.3.2.1 def pubd.main()

Definition at line 174 of file pubd.py.

9.3.3 Variable Documentation

9.3.3.1 pubd.cfg_file = "pubd.conf"

Definition at line 155 of file pubd.py.

9.3.3.2 pubd.profile = False

Definition at line 156 of file pubd.py.

9.4 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 `bpxi_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`,

9.4.1 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 roottd.py [ { -c | --config } configfile ] [ { -h | --help } ]
```

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

```
$Id: roottd.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.

9.4.2 Function Documentation

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

Definition at line 175 of file rootd.py.

9.4.2.2 def rootd.del_subject_cert ()

Definition at line 72 of file rootd.py.

9.4.2.3 def rootd.del_subject_pkcs10 ()

Definition at line 91 of file rootd.py.

9.4.2.4 def rootd.get_root_cert ()

Definition at line 48 of file rootd.py.

9.4.2.5 def rootd.get_subject_cert ()

Definition at line 56 of file rootd.py.

9.4.2.6 def rootd.get_subject_pkcs10 ()

Definition at line 77 of file rootd.py.

9.4.2.7 def rootd.issue_subject_cert_maybe (new_pkcs10)

Definition at line 98 of file rootd.py.

9.4.2.8 def rootd.root_newer_than_subject ()

Definition at line 53 of file rootd.py.

9.4.2.9 def rootd.set_subject_cert (cert)

Definition at line 65 of file rootd.py.

9.4.2.10 def rootd.set_subject_pkcs10 (pkcs10)

Definition at line 85 of file rootd.py.

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

Definition at line 238 of file rootd.py.

9.4.3 Variable Documentation**9.4.3.1 tuple rootd.bpki_ta = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))**

Definition at line 288 of file rootd.py.

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

Definition at line 284 of file rootd.py.

9.4.3.3 rootd.cfg_file = "rootd.conf"

Definition at line 268 of file rootd.py.

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

Definition at line 292 of file rootd.py.

9.4.3.5 tuple rootd.client_ta = (bpki_ta, child_bpki_cert)

Definition at line 316 of file rootd.py.

9.4.3.6 rootd.handlers = up_down_handler)

Definition at line 319 of file rootd.py.

9.4.3.7 roottd.host = https_server_host,

Definition at line 317 of file roottd.py.

9.4.3.8 tuple roottd.https_server_host = cfg.get("server-host", "")

Definition at line 294 of file roottd.py.

9.4.3.9 tuple roottd.https_server_port = int(cfg.get("server-port"))

Definition at line 295 of file roottd.py.

9.4.3.10 roottd.port = https_server_port,

Definition at line 318 of file roottd.py.

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

Definition at line 290 of file roottd.py.

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

Definition at line 291 of file roottd.py.

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

Definition at line 289 of file roottd.py.

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

Definition at line 300 of file rootd.py.

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

Definition at line 297 of file rootd.py.

9.4.3.16 rootd.rpki_root_cert = None

Definition at line 46 of file rootd.py.

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

Definition at line 303 of file rootd.py.

9.4.3.18 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.

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

Definition at line 307 of file rootd.py.

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

Definition at line 299 of file rootd.py.

```
9.4.3.21 tuple roottd.rpki_root_key = rpki.x509.RSA( Auto_file =
    cfg.get("rpki-root-key"))
```

Definition at line 302 of file roottd.py.

```
9.4.3.22 tuple roottd.rpki_root_manifest = cfg.get("rpki-root-manifest",
    "Root.mnf")
```

Definition at line 306 of file roottd.py.

```
9.4.3.23 tuple roottd.rpki_subject_cert = cfg.get("rpki-subject-cert",
    "Child.cer")
```

Definition at line 308 of file roottd.py.

```
9.4.3.24 tuple roottd.rpki_subject_lifetime =
    rpki.sundial.timedelta.parse(cfg.get("rpki-subject-
        lifetime", "30d"))
```

Definition at line 311 of file roottd.py.

```
9.4.3.25 tuple roottd.rpki_subject_pkcs10 = cfg.get("rpki-subject-pkcs10",
    "Child.pkcs10")
```

Definition at line 309 of file roottd.py.

```
9.4.3.26 tuple roottd.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 roottd.py.

9.4.3.27 rootd.server_cert = rootd_bpki_cert,

Definition at line 315 of file rootd.py.

9.5 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 [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](#)

9.6 Package rpki.__doc__

9.7 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`

9.7.1 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.

9.7.2 Function Documentation

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

Signal handler for `event_loop()`.

Definition at line 269 of file `async.py`.

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

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

Definition at line 250 of file async.py.

**9.7.2.3 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.

9.7.2.4 def rpki.async.exit_event_loop ()

Force exit from `event_loop()`.

Definition at line 364 of file async.py.

9.7.2.5 def rpki.async.run_deferred ()

Run deferred actions.

Definition at line 256 of file async.py.

9.7.3 Variable Documentation**9.7.3.1 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.

9.7.3.2 rpki::async.ExitNow = asyncore.ExitNow

Definition at line 24 of file `async.py`.

9.8 Package rpki.cli

Classes

- class [Cmd](#)

Functions

- def [yes_or_no](#)

Variables

- dictionary [_yes_or_no_prompts](#)
- [have_readline](#) = True

9.8.1 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.

9.8.2 Function Documentation

9.8.2.1 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.

9.8.3 Variable Documentation

9.8.3.1 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.

9.8.3.2 rpki::cli.have_readline = True

Definition at line 25 of file cli.py.

9.9 Package rpki.config

Classes

- class [parser](#)

9.9.1 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.

9.10 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 [DBConsistencyError](#)
- class [DERObjectConversionError](#)
- class [DuplicateObject](#)
- class [EmptyPEM](#)
- class [EmptyROAPrefixList](#)

- class [ForbiddenURI](#)
- class [HandleTranslationError](#)
- class [HTTPRequestFailed](#)
- class [HTTPSBadVersion](#)
- class [HTTPSClientAborted](#)
- class [HTTPSUnexpectedState](#)
- class [MissingCMSCRL](#)
- class [MissingCMSEcert](#)
- 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 [TLSValidationException](#)
- class [UnexpectedCMSCerts](#)
- class [UnexpectedCMSCRLs](#)
- class [UnparseableCMSDER](#)
- class [UpstreamError](#)
- class [WrongEContentType](#)

9.10.1 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.

9.11 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.

9.11.1 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.

9.11.2 Function Documentation

9.11.2.1 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 tomorrow is nobody else's business.

Definition at line 1094 of file https.py.

9.11.2.2 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.

9.11.2.3 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.

9.11.2.4 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.

9.11.3 Variable Documentation

9.11.3.1 `rpki::https::client_queues = {}`

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

Definition at line 1032 of file https.py.

9.11.3.2 `rpki::https::debug_http = False`

Verbose chatter about HTTP streams.

Definition at line 45 of file https.py.

9.11.3.3 `rpki::https::debug_tls_certs = False`

Verbose chatter about TLS certificates.

Definition at line 49 of file https.py.

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

Default HTTP client connection timeout.

Definition at line 61 of file https.py.

9.11.3.5 `rpki::https::default_http_version = (1, 0)`

Preferred HTTP version.

Definition at line 72 of file https.py.

9.11.3.6 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.

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

HTTP content type used for all RPKI messages.

Definition at line 41 of file https.py.

9.11.3.8 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.

9.11.3.9 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.

9.11.3.10 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.

9.12 Package rpki.ipaddrs

Classes

- class [v4addr](#)
- class [v6addr](#)

9.12.1 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.

9.13 Package rpk.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

9.13.1 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.

9.13.2 Variable Documentation

9.13.2.1 rpki::left_right.enforce_strict_up_down_xml_sender = False

Definition at line 40 of file left_right.py.

9.14 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)`

9.14.1 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.
```

9.14.2 Function Documentation

9.14.2.1 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.

9.14.2.2 def rpki.log.set_trace (enable)

Enable or disable call tracing.

Definition at line 63 of file log.py.

9.14.2.3 def rpki.log.trace ()

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

Definition at line 91 of file log.py.

9.14.2.4 def rpki.log.traceback ()

Consolidated backtrace facility with a bit of extra info.

Definition at line 100 of file log.py.

9.14.3 Variable Documentation**9.14.3.1 tuple rpki::log.debug = logger(syslog.LOG_DEBUG)**

Definition at line 89 of file log.py.

9.14.3.2 rpki::log::enable_trace = False

Whether call tracing is enabled.

Definition at line 41 of file log.py.

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

Definition at line 85 of file log.py.

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

Definition at line 88 of file log.py.

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

Definition at line 87 of file log.py.

9.14.3.6 int rpki::log.pid = 0

Definition at line 49 of file log.py.

9.14.3.7 string rpki::log.tag = ""

Definition at line 48 of file log.py.

9.14.3.8 rpki::log::use_syslog = True

Whether to use syslog.

Definition at line 46 of file log.py.

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

Definition at line 86 of file log.py.

9.15 Package rpki.manifest

Classes

- class [FileAndHash](#)
- class [FilesAndHashes](#)
- class [Manifest](#)

9.15.1 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.

9.16 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.

9.16.1 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.

9.16.2 Variable Documentation

9.16.2.1 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.

9.16.2.2 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.

9.17 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](#)

9.17.1 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.

9.18 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.

9.18.1 Variable Documentation

9.18.1.1 rpki::relaxng::left_right

Parsed RelaxNG [left_right](#) schema.

Definition at line 7 of file relaxng.py.

9.18.1.2 rpki::relaxng::publication

Parsed RelaxNG publication schema.

Definition at line 1252 of file relaxng.py.

9.18.1.3 rpki::relaxng::up_down

Parsed RelaxNG [up_down](#) schema.

Definition at line 998 of file relaxng.py.

9.19 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.

9.19.1 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.

9.19.2 Function Documentation

9.19.2.1 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.

9.19.2.2 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.

9.19.2.3 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.

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

Definition at line 884 of file resource_set.py.

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

Definition at line 917 of file resource_set.py.

9.19.3 Variable Documentation**9.19.3.1 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.

9.20 Package rpki.roa**Classes**

- class [ROAIPAddress](#)
- class [ROAIPAddresses](#)
- class [ROAIPAddressFamilies](#)
- class [ROAIPAddressFamily](#)
- class [RouteOriginAttestation](#)

9.20.1 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
```

9.21 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](#)

9.21.1 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.

9.22 Package rpki.sql

Classes

- class [session](#)
- class [sql_persistent](#)
- class [template](#)

9.22.1 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.

9.23 Package rpkisundial

Classes

- class [datetime](#)
- class [timedelta](#)

Functions

- def [_cast](#)
- def [now](#)
- def [test](#)

9.23.1 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.
```

9.23.2 Function Documentation

9.23.2.1 def rpkisundial._cast (x) [private]

Cast result of arithmetic operations back into correct subtype.

Definition at line 257 of file sundial.py.

9.23.2.2 def rpkisundial.now ()

Get current timestamp.

Definition at line 50 of file sundial.py.

9.23.2.3 def rpki.sundial.test (t)

Definition at line 269 of file sundial.py.

9.24 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/"

9.24.1 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.

9.24.2 Variable Documentation

9.24.2.1 `dictionary rpki::up_down.nsmap = { None : xmlns }`

Definition at line 41 of file up_down.py.

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

Definition at line 39 of file up_down.py.

9.25 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

9.25.1 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.

9.25.2 Function Documentation

9.25.2.1 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.

9.25.2.2 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.

9.25.2.3 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.

9.26 Package rpki.xml_utils

Classes

- class [base_elt](#)
- class [data_elt](#)
- class [msg](#)
- class [sax_handler](#)
- class [text_elt](#)

9.26.1 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.
```

9.27 Package rpkid

Functions

- def [main](#)

Variables

- string [cfg_file](#) = "rpkid.conf"
- [profile](#) = None

9.27.1 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 } outfile ]  
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.
```

9.27.2 Function Documentation

9.27.2.1 def rpkid.main ()

Definition at line 68 of file rpkid.py.

9.27.3 Variable Documentation

9.27.3.1 rpkid.cfg_file = "rpkid.conf"

Definition at line 49 of file rpkid.py.

9.27.3.2 rpkid.profile = None

Definition at line 50 of file rpkid.py.

10 Class Documentation

10.1 async_chat Class Reference

Inherited by [rpki.https.http_stream](#).

The documentation for this class was generated from the following file:

- [https.py \(3191\)](#)

10.2 dispatcher Class Reference

Inherited by [rpki.https.http_listener](#).

The documentation for this class was generated from the following file:

- [https.py \(3191\)](#)

10.3 Cmd Class Reference

Inherited by [rpki.cli.Cmd](#).

The documentation for this class was generated from the following file:

- [cli.py \(3191\)](#)

10.4 Exception Class Reference

Inherited by [rpki.exceptions.RPKI_Exception](#).

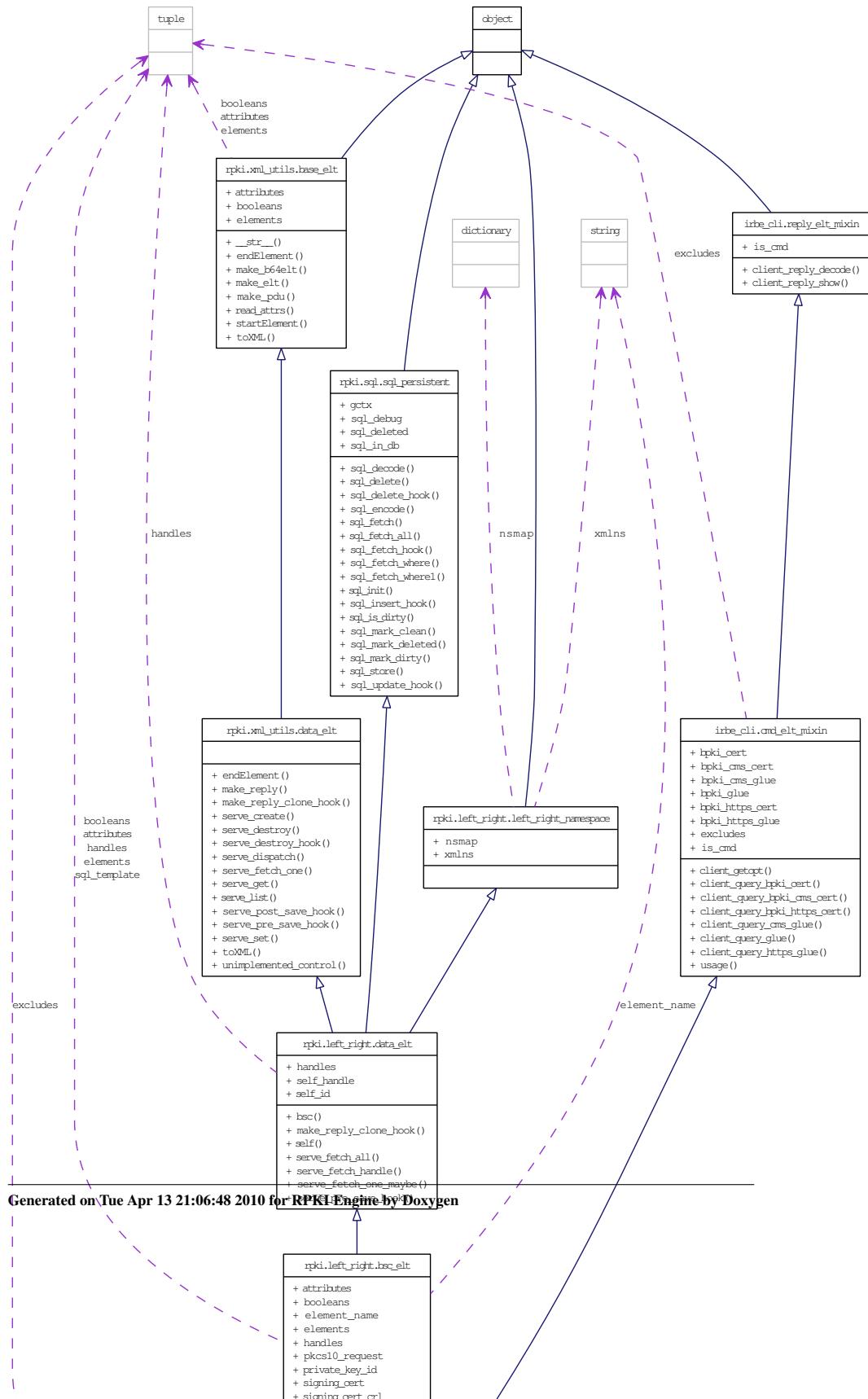
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.5 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.

10.5.1 Detailed Description

Definition at line 152 of file irbe_cli.py.

10.5.2 Member Function Documentation

10.5.2.1 def irbe_cli.bsc_elt.client_query_signing_cert (*self*, *arg*)

--signing_cert option.

Definition at line 156 of file irbe_cli.py.

10.5.2.2 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.

10.5.2.3 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](#).

10.5.3 Member Data Documentation**10.5.3.1 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](#).

10.5.3.2 irbe_cli.bsc_elt.signing_cert

Reimplemented from [rpki.left_right.bsc_elt](#).

Definition at line 158 of file [irbe_cli.py](#).

10.5.3.3 irbe_cli.bsc_elt.signing_cert_crl

Reimplemented from [rpki.left_right.bsc_elt](#).

Definition at line 162 of file [irbe_cli.py](#).

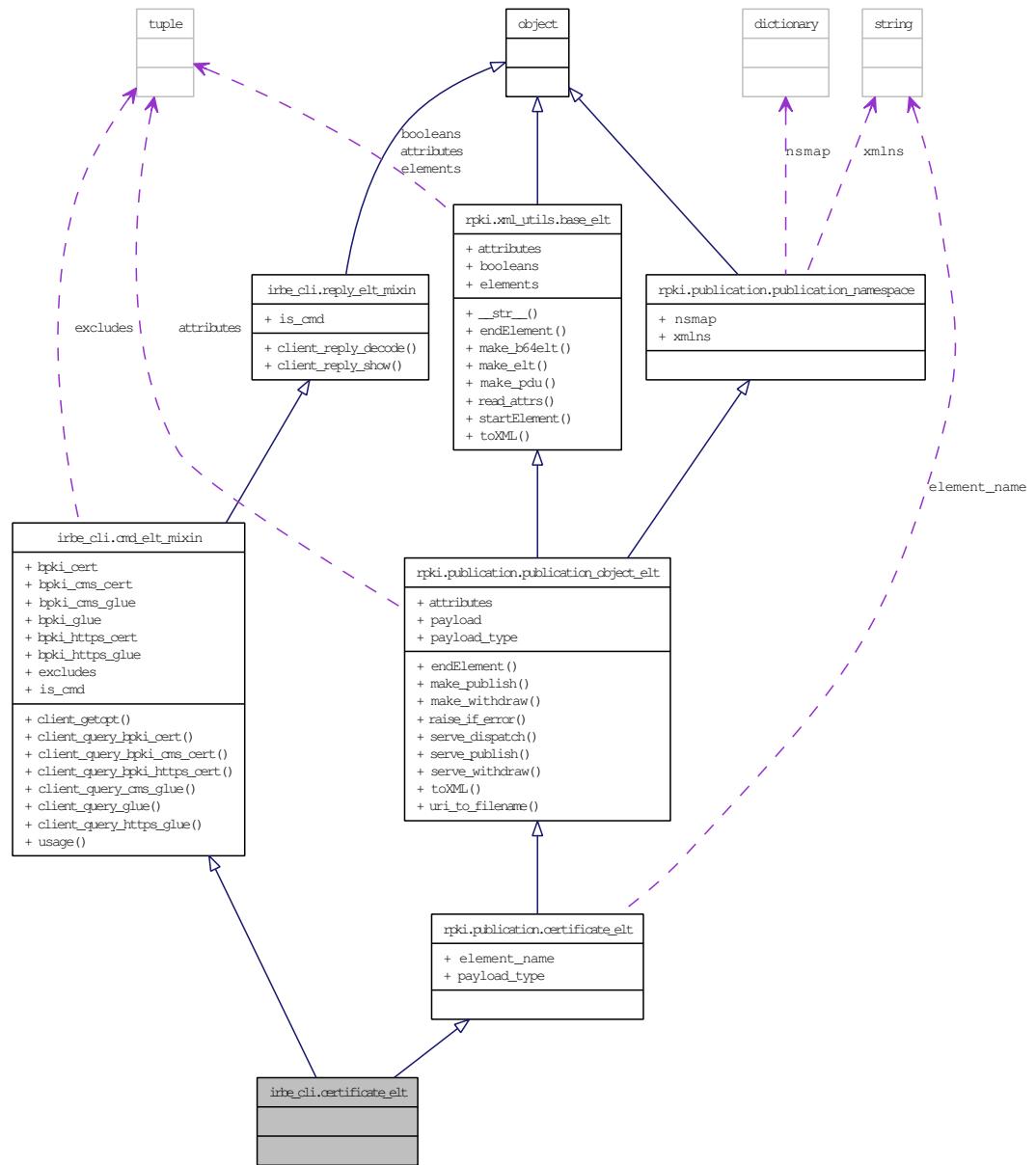
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.6 irbe_cli.certificate_elt Class Reference

Inherits [irbe_cli::cmd_elt_mixin](#), and [rpki::publication::certificate_elt](#).

Collaboration diagram for irbe_cli.certificate_elt:



10.6.1 Detailed Description

Definition at line 211 of file `irbe_cli.py`.

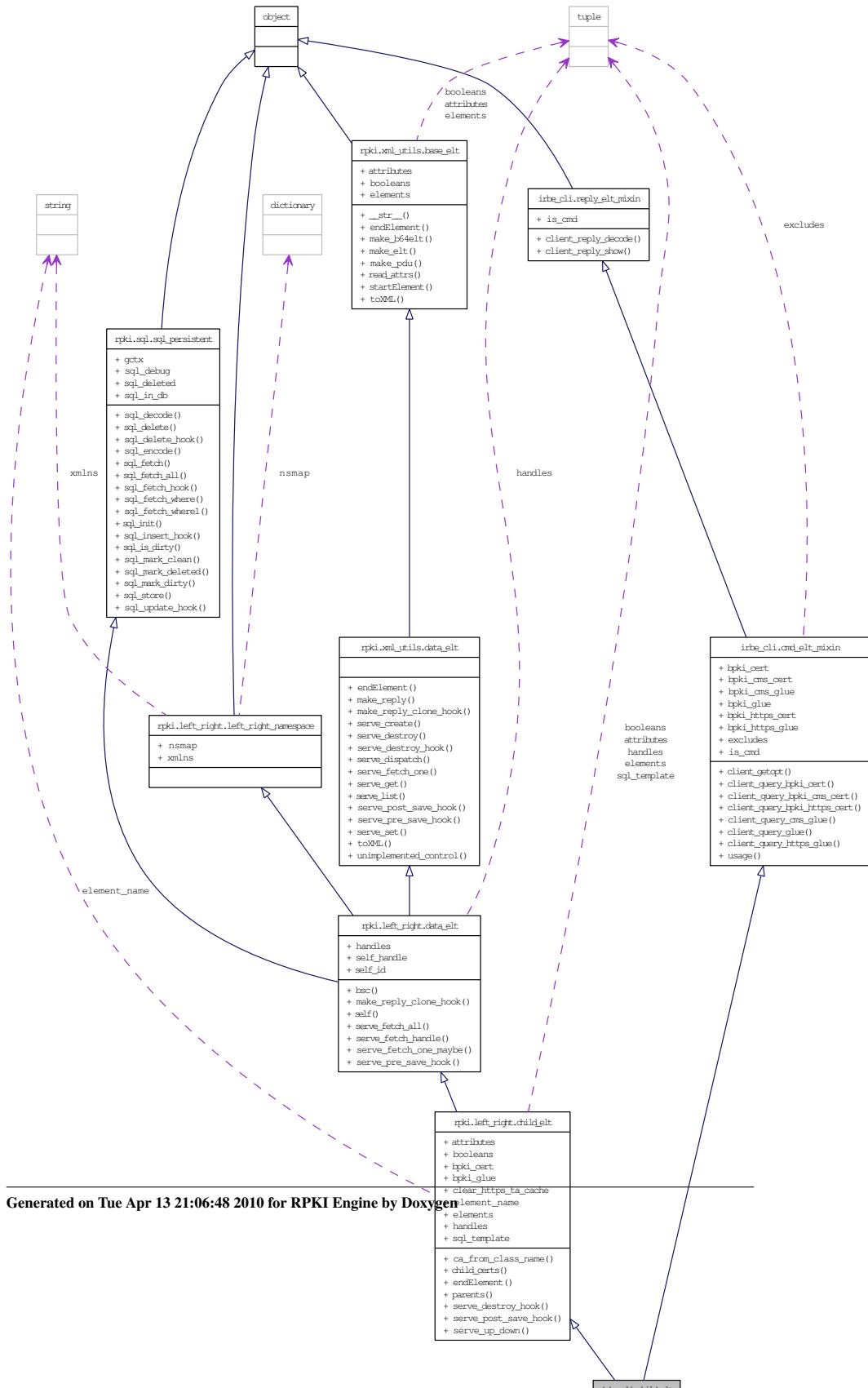
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.7 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:



10.7.1 Detailed Description

Definition at line 174 of file [irbe_cli.py](#).

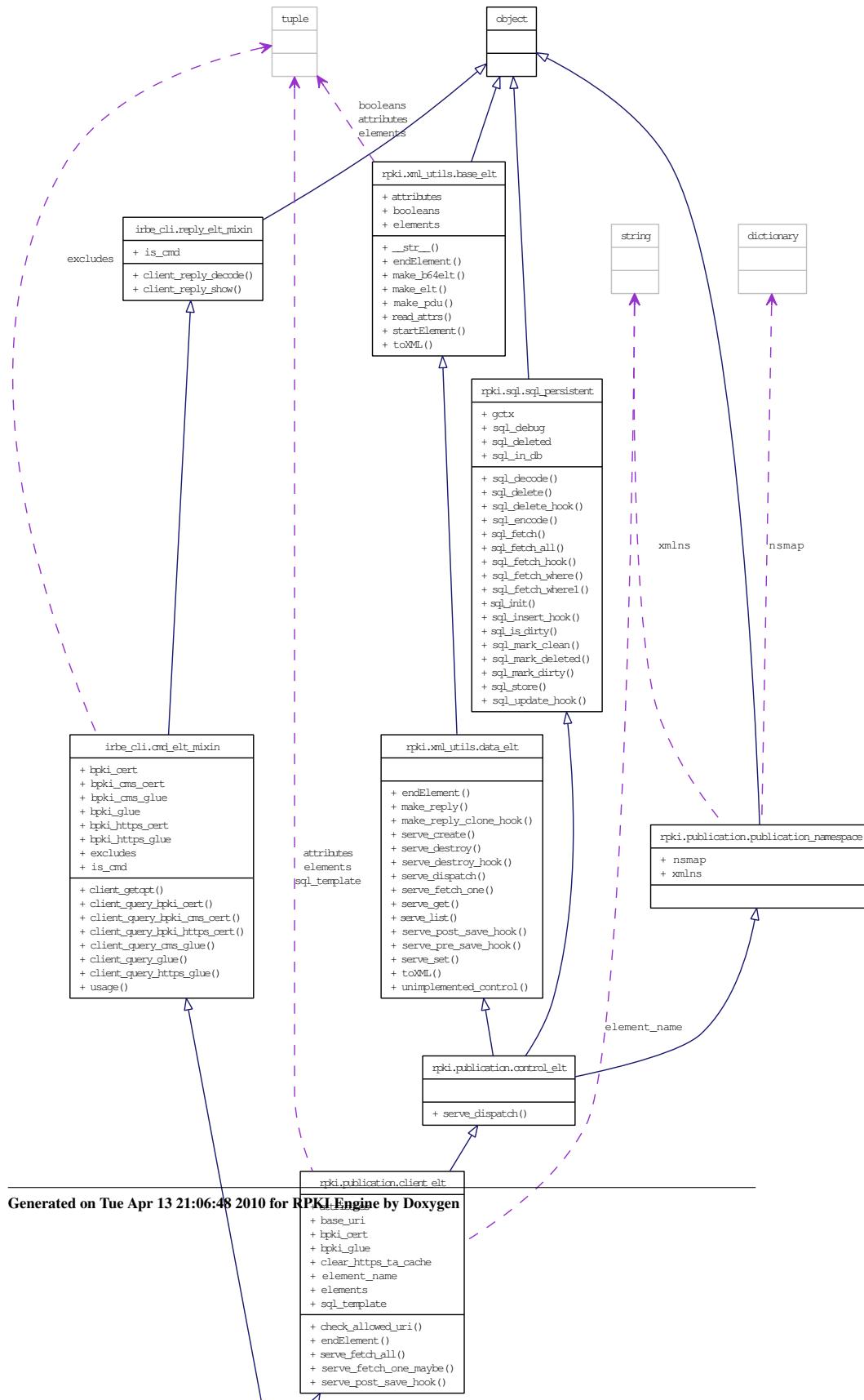
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.8 irbe_cli.client_elt Class Reference

Inherits [irbe_cli::cmd_elt_mixin](#), and [rpki::publication::client_elt](#).

Collaboration diagram for irbe_cli.client_elt:



10.8.1 Detailed Description

Definition at line 208 of file irbe_cli.py.

The documentation for this class was generated from the following file:

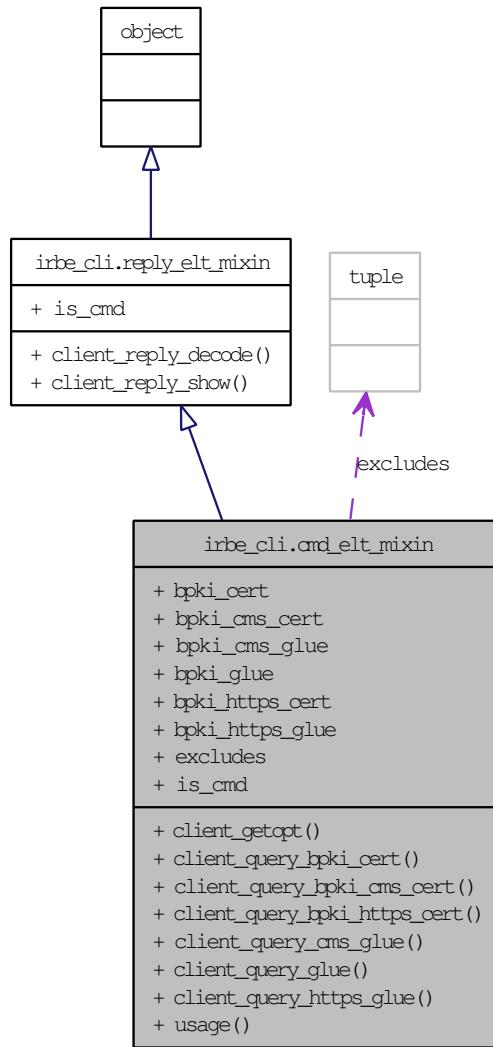
- [irbe_cli.py \(3107\)](#)

10.9 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_bpkı_cert`
- def `client_query_bpkı_cms_cert`
- def `client_query_bpkı_https_cert`
- def `client_query_cms_glue`

- def `client_query_glue`
- def `client_query_https_glue`
- def `usage`

Public Attributes

- `bpkı_cert`
- `bpkı_cms_cert`
- `bpkı_cms_glue`
- `bpkı_glue`
- `bpkı_https_cert`
- `bpkı_https_glue`

Static Public Attributes

- tuple `excludes` = ()
XML attributes and elements that should not be allowed as command line arguments.
- `is_cmd` = True

10.9.1 Detailed Description

Protocol mix-in for command line client element PDUs.

Definition at line 68 of file irbe_cli.py.

10.9.2 Member Function Documentation

10.9.2.1 def `irbe_cli.cmd_elt_mixin.client_getopt (self, argv)`

Parse options for this class.

Definition at line 92 of file irbe_cli.py.

10.9.2.2 def `irbe_cli.cmd_elt_mixin.client_query_bpkı_cert (self, arg)`

Special handler for --bpki_cert option.

Definition at line 109 of file irbe_cli.py.

10.9.2.3 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.

10.9.2.4 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.

10.9.2.5 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.

10.9.2.6 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.

10.9.2.7 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.

10.9.2.8 def irbe_cli.cmd_elt_mixin.usage (cls)

Generate usage message for this PDU.

Definition at line 81 of file irbe_cli.py.

10.9.3 Member Data Documentation**10.9.3.1 irbe_cli.cmd_elt_mixin.bpk_i_cert**

Definition at line 111 of file irbe_cli.py.

10.9.3.2 irbe_cli.cmd_elt_mixin.bpk_i_cms_cert

Definition at line 119 of file irbe_cli.py.

10.9.3.3 irbe_cli.cmd_elt_mixin.bpk_i_cms_glue

Definition at line 123 of file irbe_cli.py.

10.9.3.4 irbe_cli.cmd_elt_mixin.bpk_i_glue

Definition at line 115 of file irbe_cli.py.

10.9.3.5 irbe_cli.cmd_elt_mixin.bpk_i_https_cert

Definition at line 127 of file irbe_cli.py.

10.9.3.6 irbe_cli.cmd_elt_mixin.bpk_i_https_glue

Definition at line 131 of file irbe_cli.py.

10.9.3.7 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.

10.9.3.8 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:

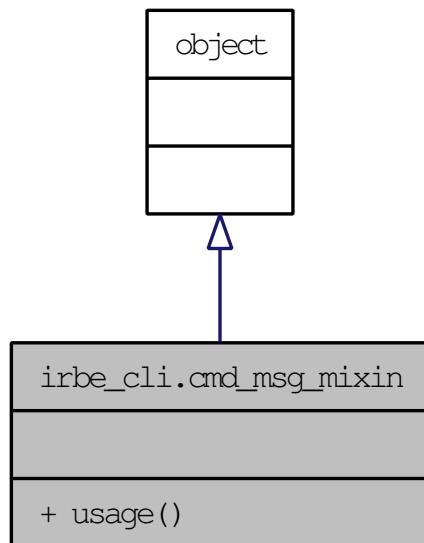
- [irbe_cli.py \(3107\)](#)

10.10 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](#)

10.10.1 Detailed Description

Protocol mix-in for command line client message PDUs.

Definition at line 133 of file irbe_cli.py.

10.10.2 Member Function Documentation

10.10.2.1 def irbe_cli.cmd_msg_mixin.usage (*cls*)

Generate usage message for this PDU.

Definition at line 139 of file irbe_cli.py.

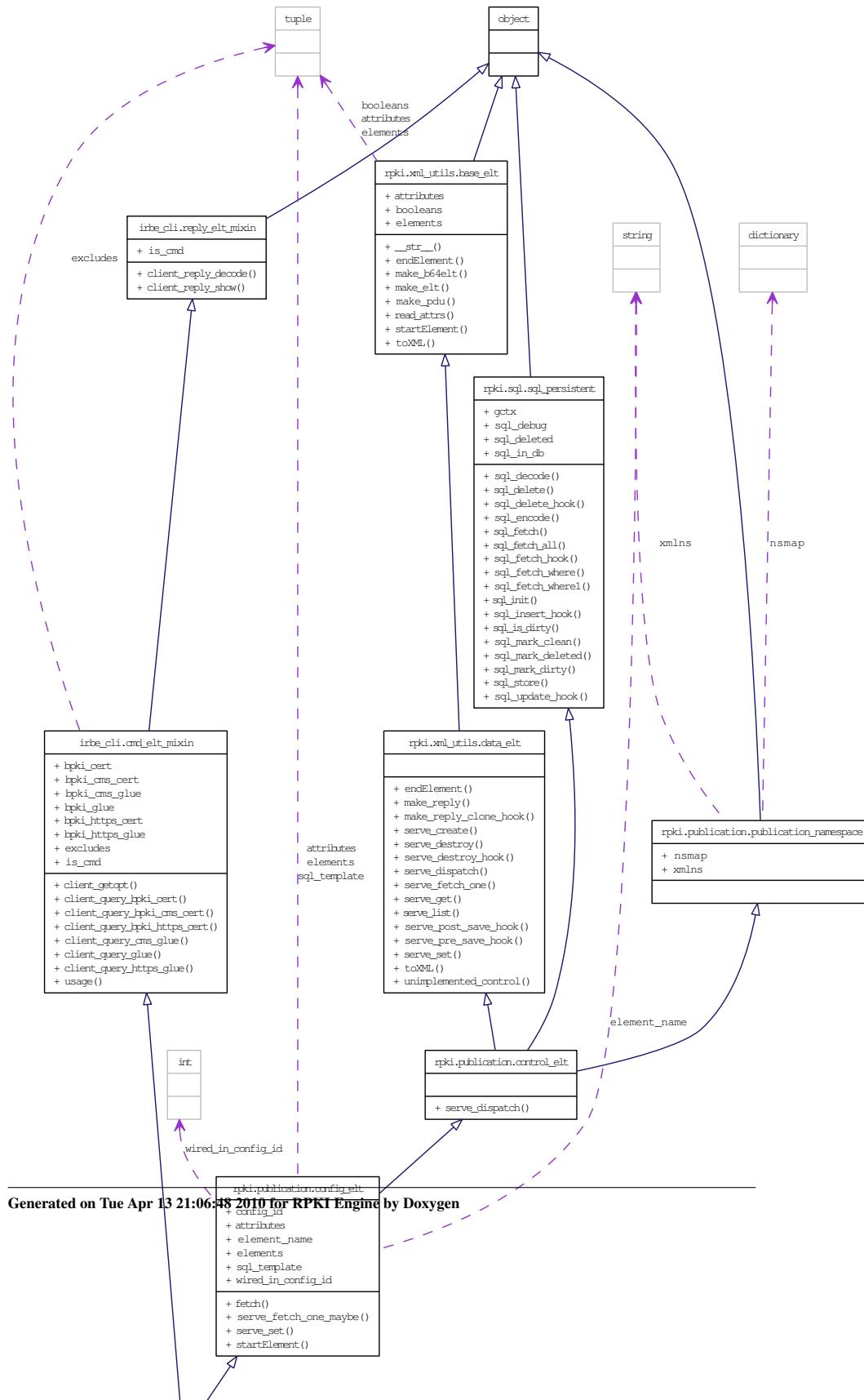
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.11 irbe_cli.config_elt Class Reference

Inherits [irbe_cli::cmd_elt_mixin](#), and [rpkim::publication::config_elt](#).

Collaboration diagram for irbe_cli.config_elt:



Public Member Functions

- def [client_query_bpki_crl](#)

Public Attributes

- [bpki_crl](#)

10.11.1 Detailed Description

Definition at line 202 of file irbe_cli.py.

10.11.2 Member Function Documentation**10.11.2.1 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.

10.11.3 Member Data Documentation**10.11.3.1 irbe_cli.config_elt.bpkicrl**

Definition at line 206 of file irbe_cli.py.

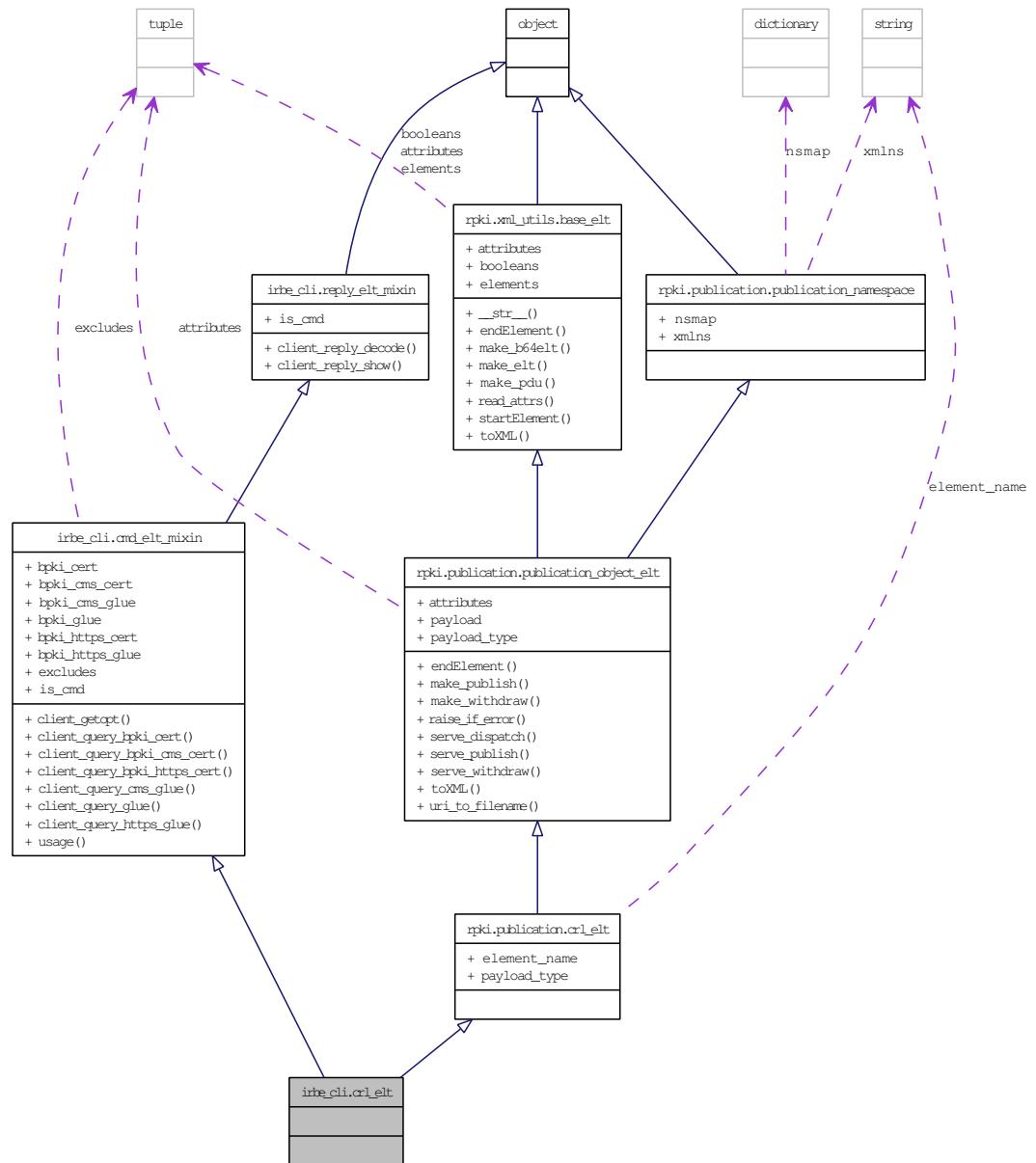
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.12 irbe_cli.crl_elt Class Reference

Inherits [irbe_cli::cmd_elt_mixin](#), and [rpki::publication::crl_elt](#).

Collaboration diagram for irbe_cli.crl_elt:



10.12.1 Detailed Description

Definition at line 214 of file `irbe_cli.py`.

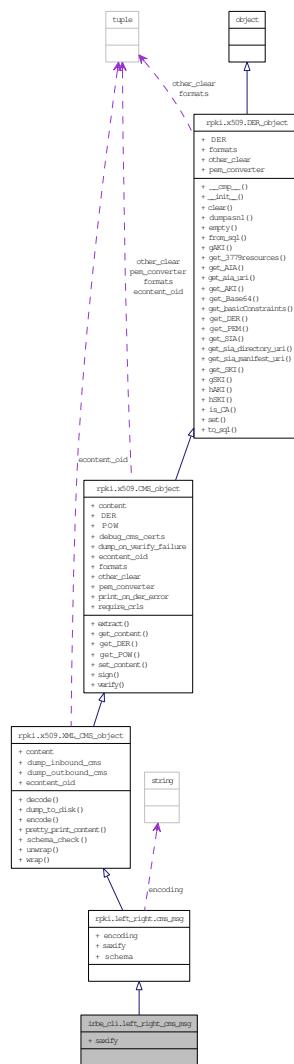
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.13 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`

10.13.1 Detailed Description

Definition at line 197 of file `irbe_cli.py`.

10.13.2 Member Data Documentation

10.13.2.1 `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`.

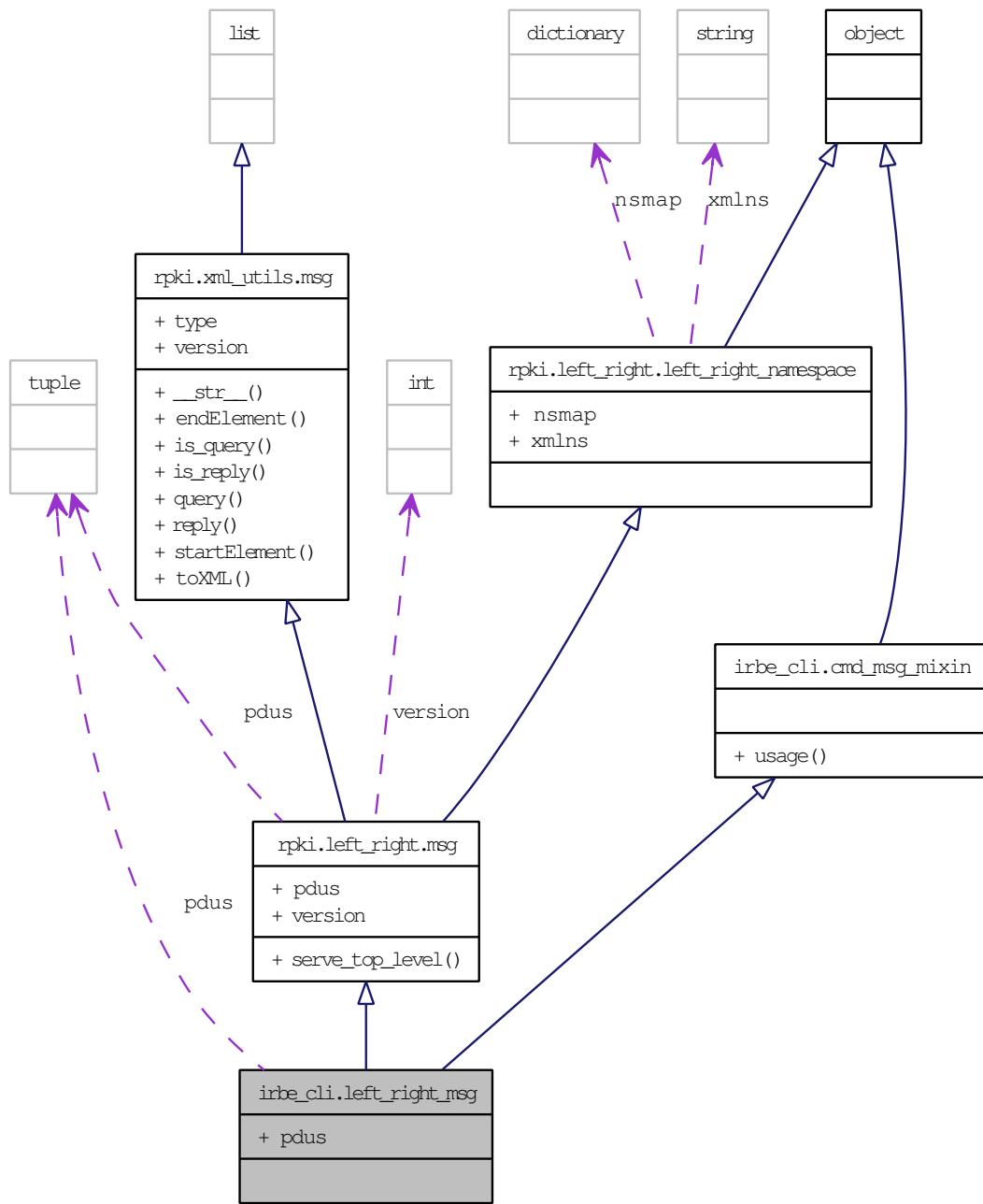
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.14 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.

10.14.1 Detailed Description

Definition at line 189 of file irbe_cli.py.

10.14.2 Member Data Documentation

10.14.2.1 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 [rpk.left_right.msg](#).

Definition at line 190 of file irbe_cli.py.

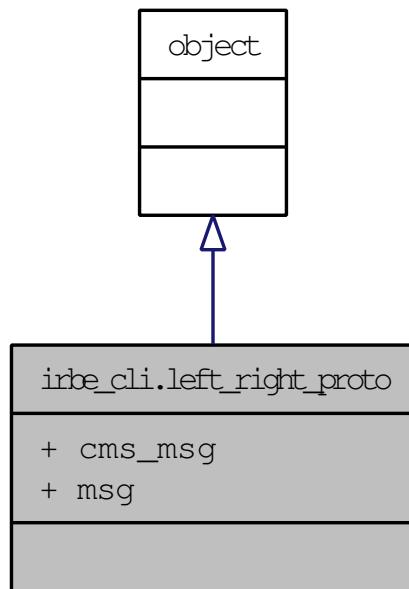
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.15 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](#)

10.15.1 Detailed Description

Definition at line 302 of file `irbe_cli.py`.

10.15.2 Member Data Documentation

10.15.2.1 `irbe_cli.left_right_proto.cms_msg = left_right_cms_msg [static]`

Definition at line 303 of file `irbe_cli.py`.

10.15.2.2 `irbe_cli.left_right_proto.msg = left_right_msg [static]`

Definition at line 304 of file irbe_cli.py.

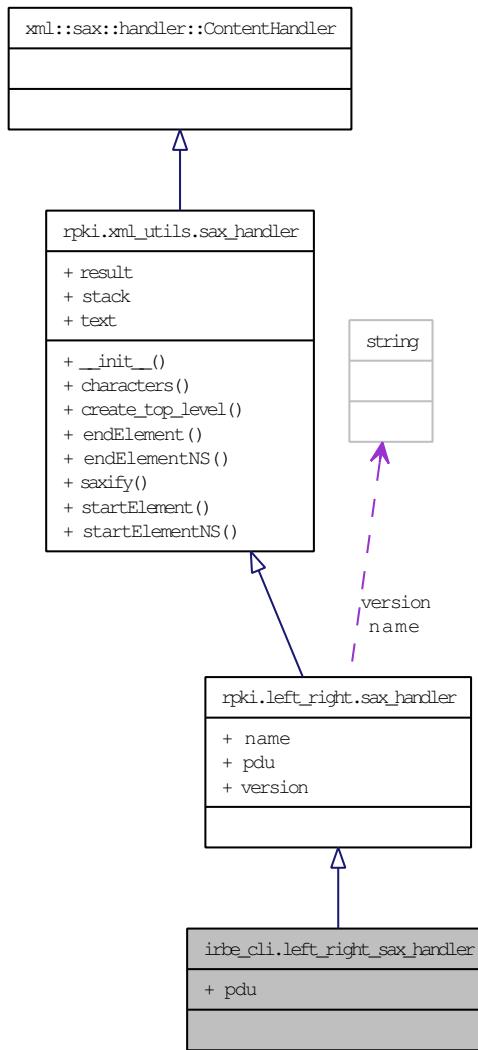
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.16 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`

10.16.1 Detailed Description

Definition at line 194 of file `irbe_cli.py`.

10.16.2 Member Data Documentation**10.16.2.1 irbe_cli.left_right_sax_handler.pdu = left_right_msg [static]**

Reimplemented from `rpkilib.left_right.sax_handler`.

Definition at line 195 of file `irbe_cli.py`.

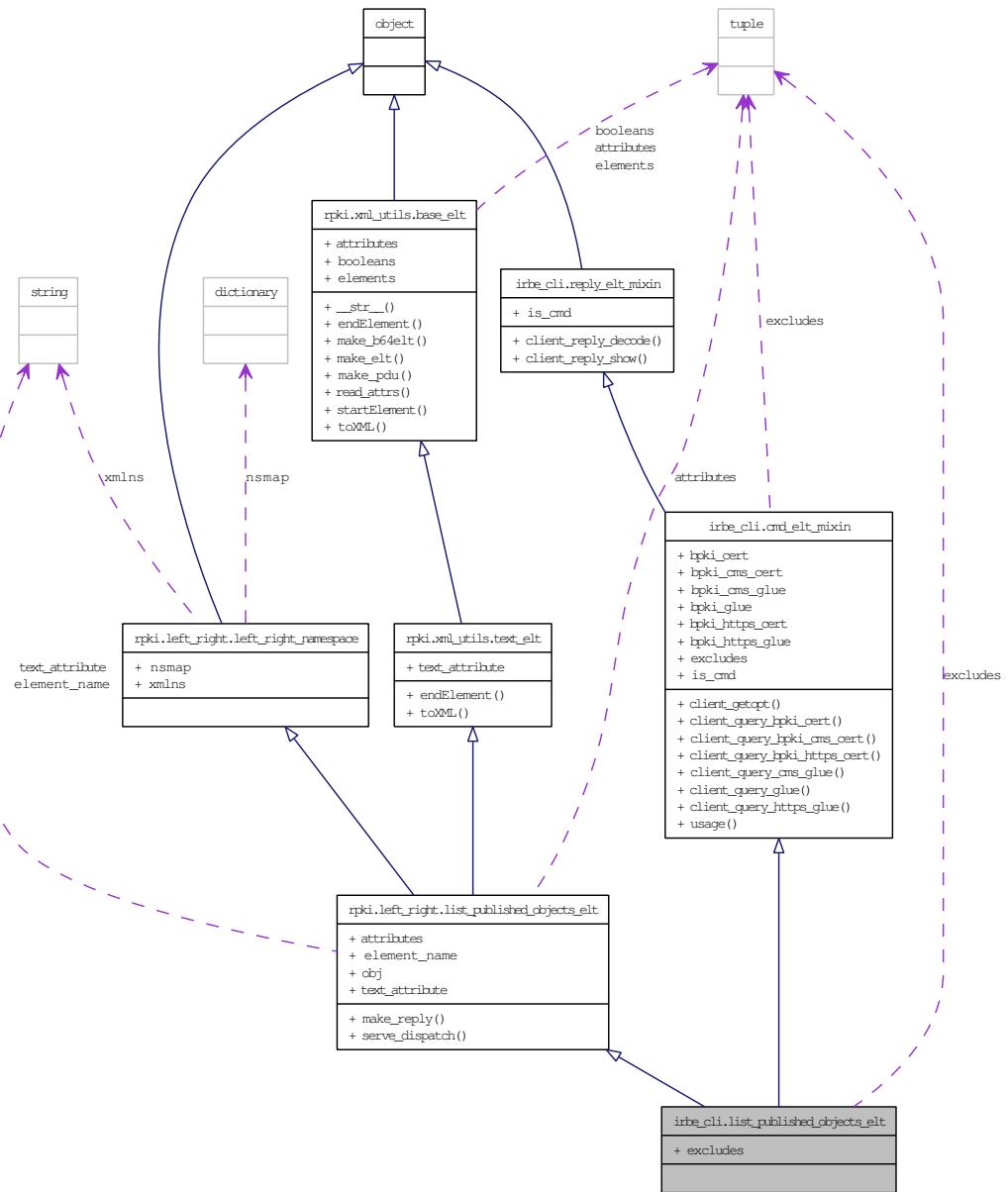
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.17 irbe_cli.list_published_objects_elt Class Reference

Inherits `irbe_cli::cmd_elt_mixin`, and `rpkilib::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.

10.17.1 Detailed Description

Definition at line 180 of file [irbe_cli.py](#).

10.17.2 Member Data Documentation

10.17.2.1 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](#).

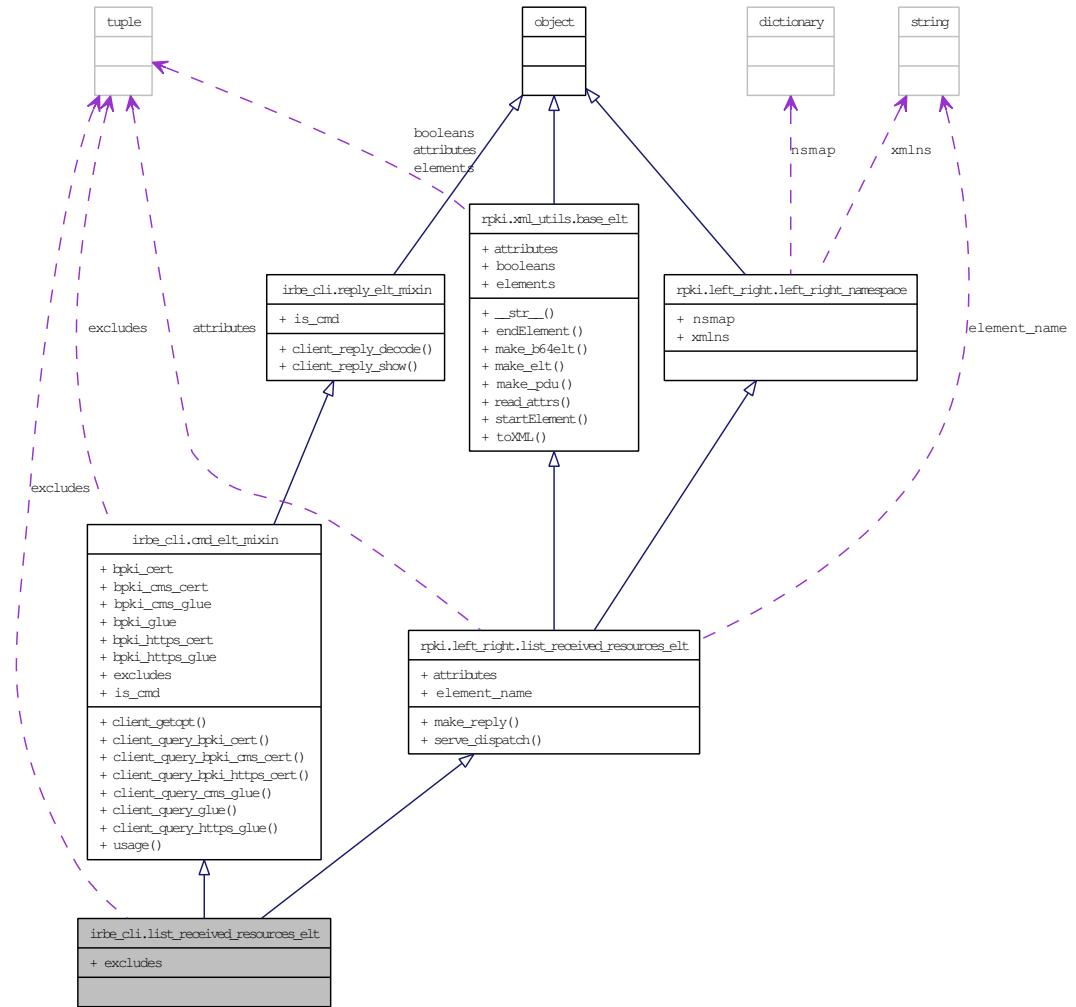
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.18 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.

10.18.1 Detailed Description

Definition at line 183 of file irbe_cli.py.

10.18.2 Member Data Documentation

**10.18.2.1 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.

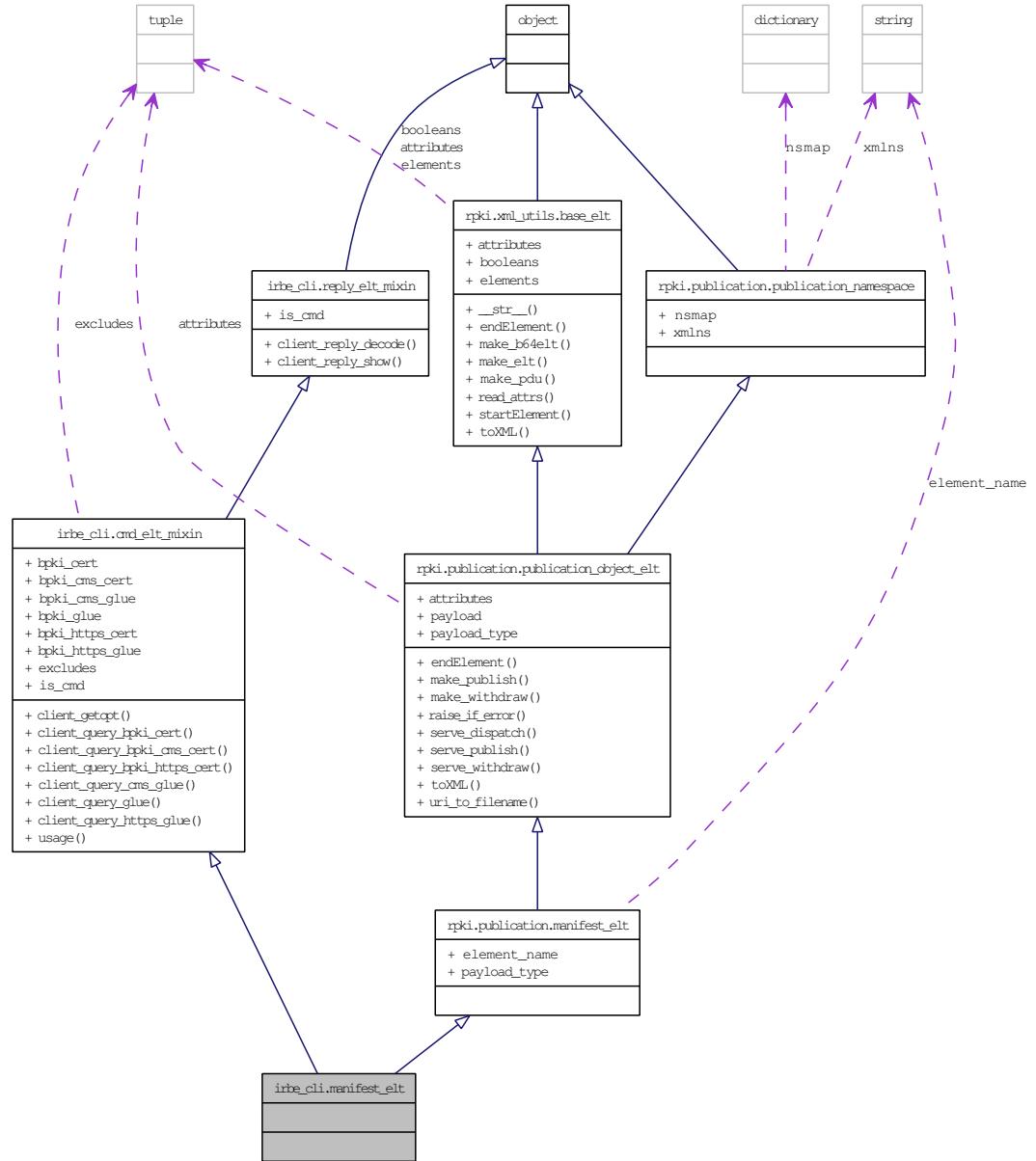
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.19 irbe_cli.manifest_elt Class Reference

Inherits [irbe_cli::cmd_elt_mixin](#), and [rpkid::publication::manifest_elt](#).

Collaboration diagram for irbe_cli.manifest_elt:



10.19.1 Detailed Description

Definition at line 217 of file `irbe_cli.py`.

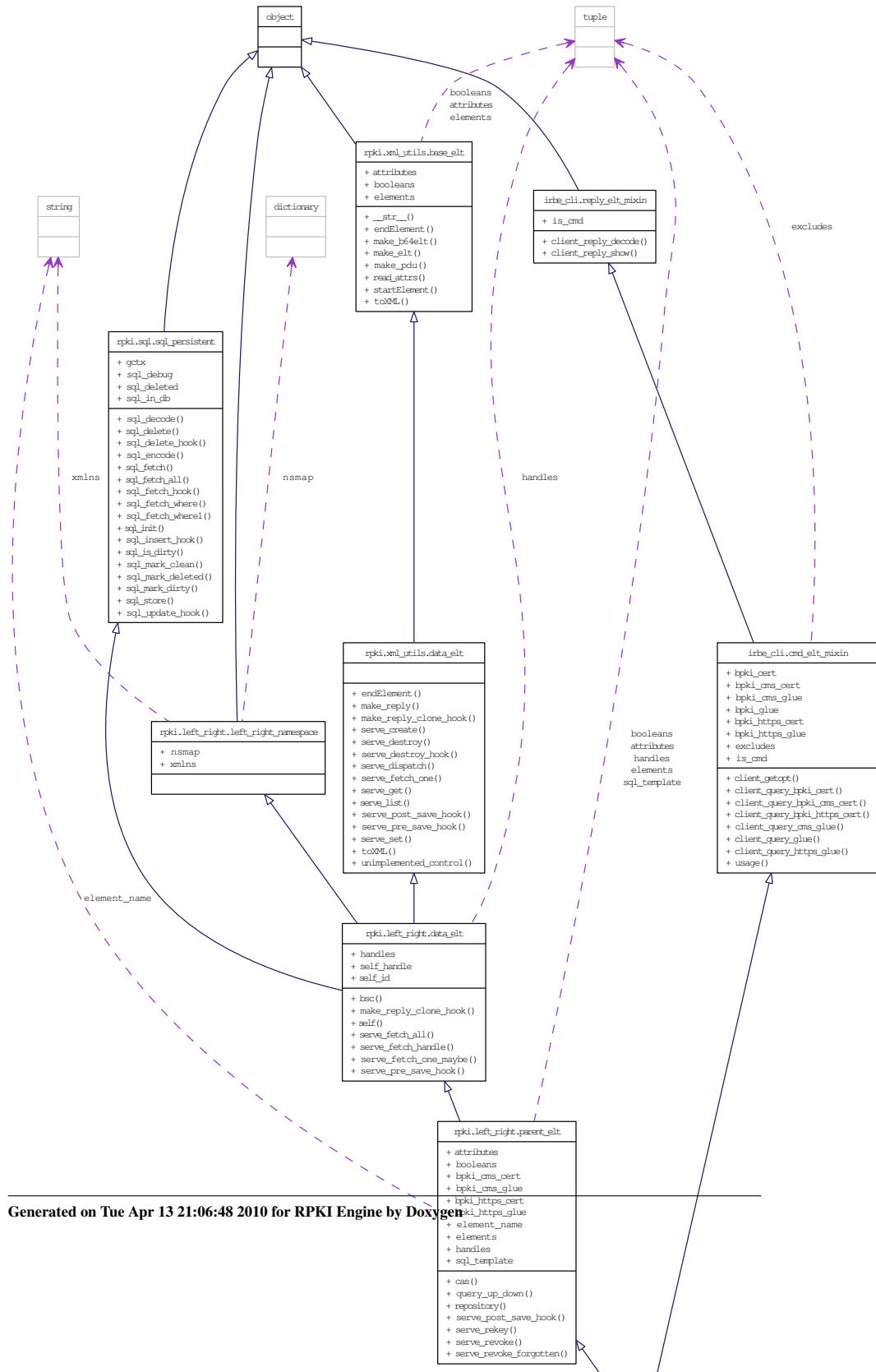
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.20 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:



10.20.1 Detailed Description

Definition at line 171 of file [irbe_cli.py](#).

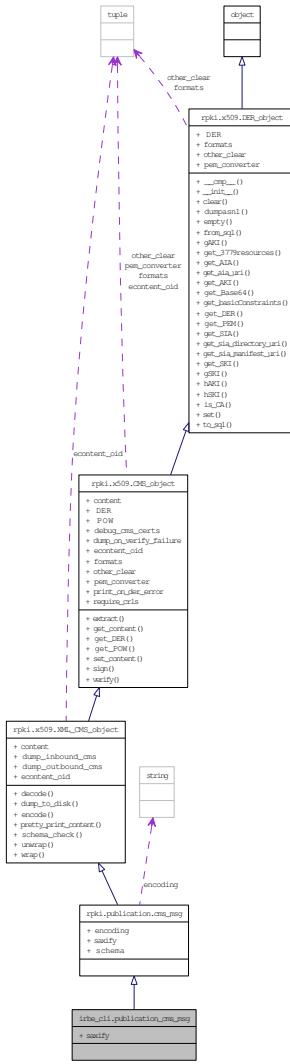
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.21 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`

10.21.1 Detailed Description

Definition at line 233 of file `irbe_cli.py`.

10.21.2 Member Data Documentation

10.21.2.1 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](#).

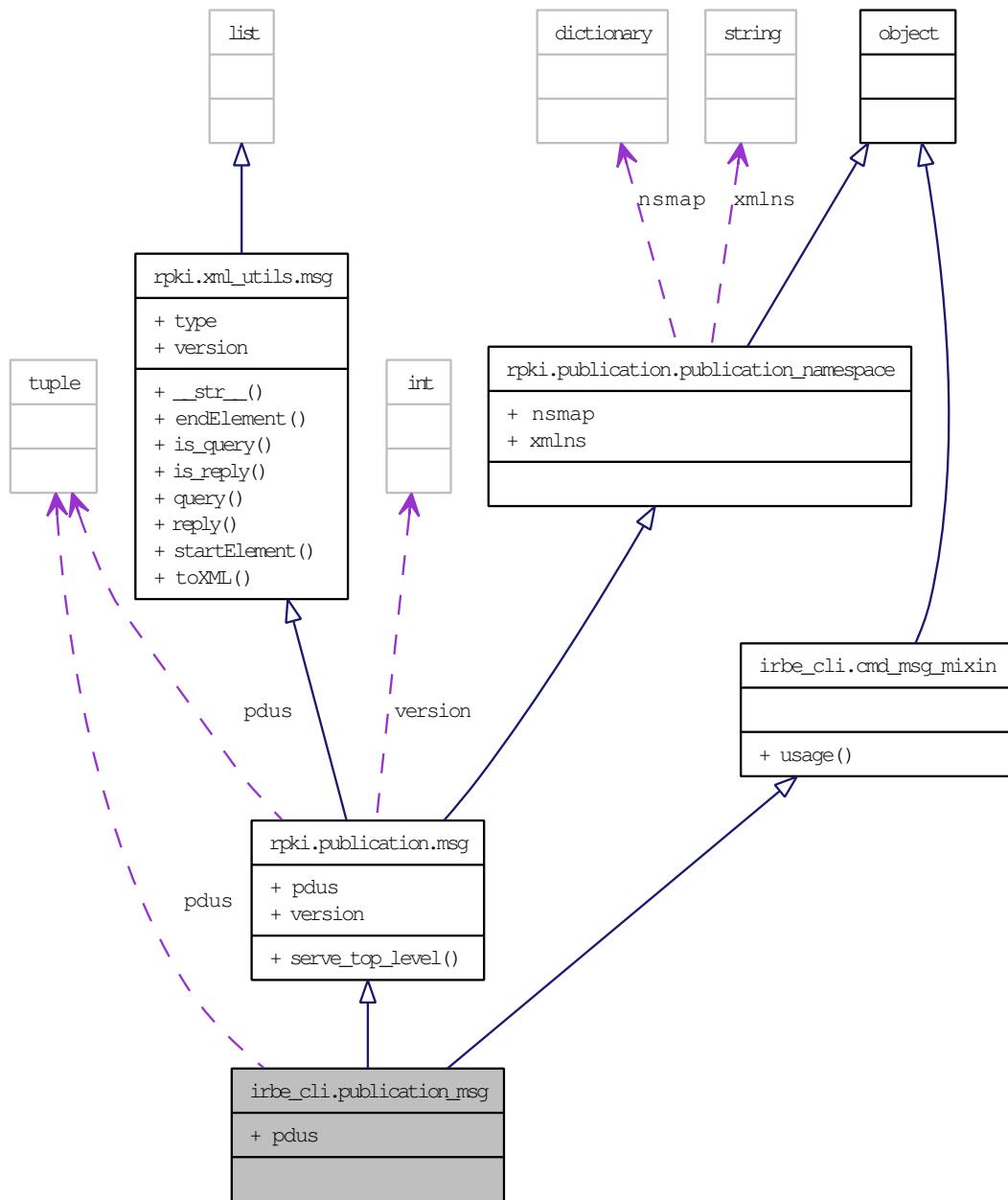
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.22 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.

10.22.1 Detailed Description

Definition at line 226 of file irbe_cli.py.

10.22.2 Member Data Documentation

10.22.2.1 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, manifest_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.

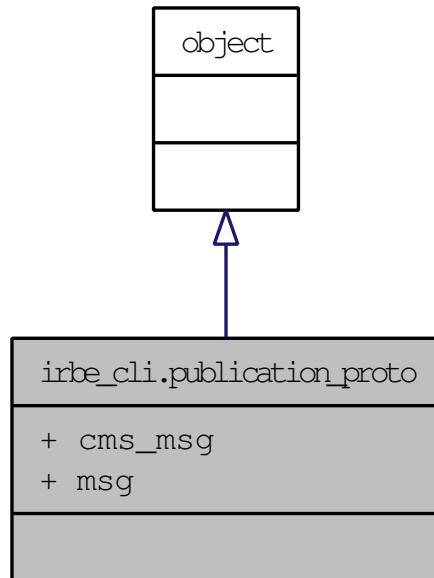
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.23 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`

10.23.1 Detailed Description

Definition at line 319 of file irbe_cli.py.

10.23.2 Member Data Documentation

10.23.2.1 `irbe_cli.publication_proto.cms_msg = publication_cms_msg [static]`

Definition at line 321 of file irbe_cli.py.

10.23.2.2 `irbe_cli.publication_proto.msg = publication_msg [static]`

Definition at line 320 of file irbe_cli.py.

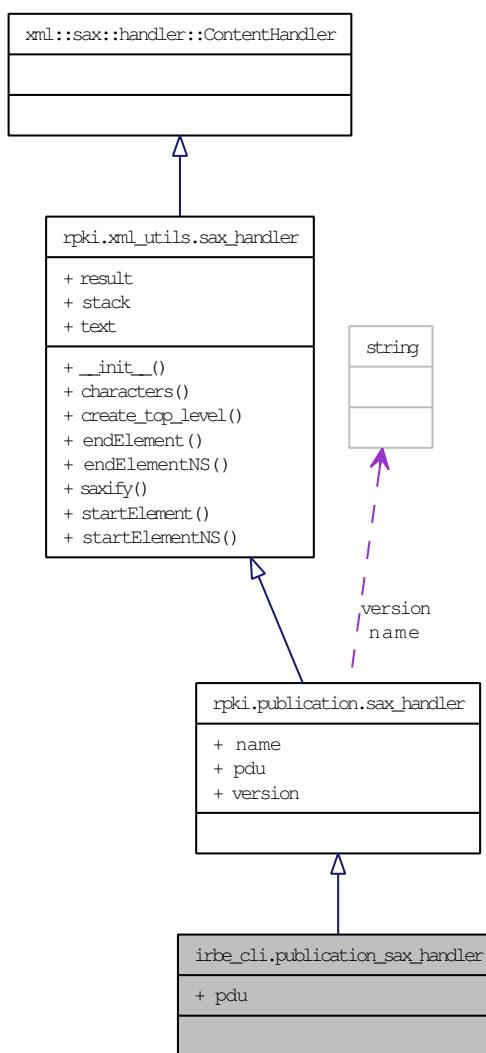
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.24 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`

10.24.1 Detailed Description

Definition at line 230 of file `irbe_cli.py`.

10.24.2 Member Data Documentation

10.24.2.1 `irbe_cli.publication_sax_handler.pdu = publication_msg [static]`

Reimplemented from `rpkি.publication.sax_handler`.

Definition at line 231 of file `irbe_cli.py`.

The documentation for this class was generated from the following file:

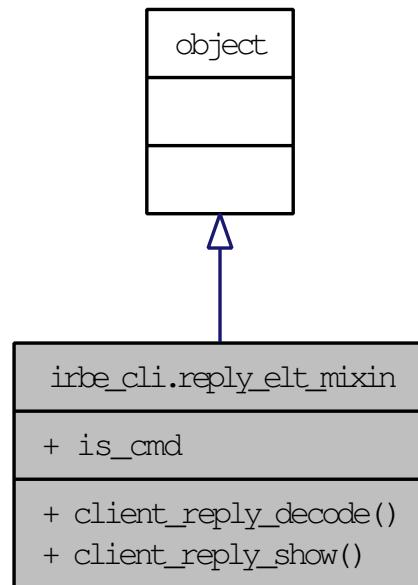
- [irbe_cli.py \(3107\)](#)

10.25 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

10.25.1 Detailed Description

Protocol mix-in for printout of reply PDUs.

Definition at line 52 of file `irbe_cli.py`.

10.25.2 Member Function Documentation

10.25.2.1 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](#).

10.25.2.2 def irbe_cli.reply_elt_mixin.client_reply_show (*self*)

Definition at line 62 of file [irbe_cli.py](#).

10.25.3 Member Data Documentation

10.25.3.1 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](#).

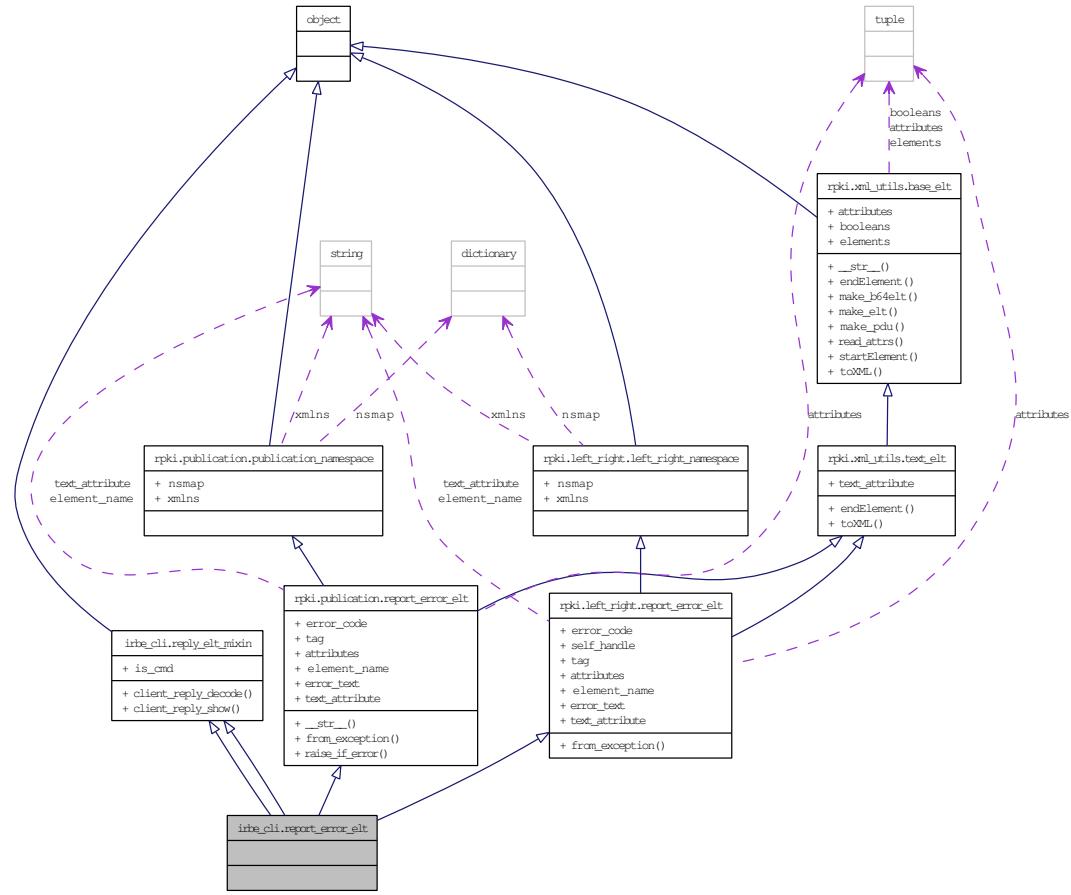
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.26 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:



10.26.1 Detailed Description

Definition at line 186 of file `irbe_cli.py`.

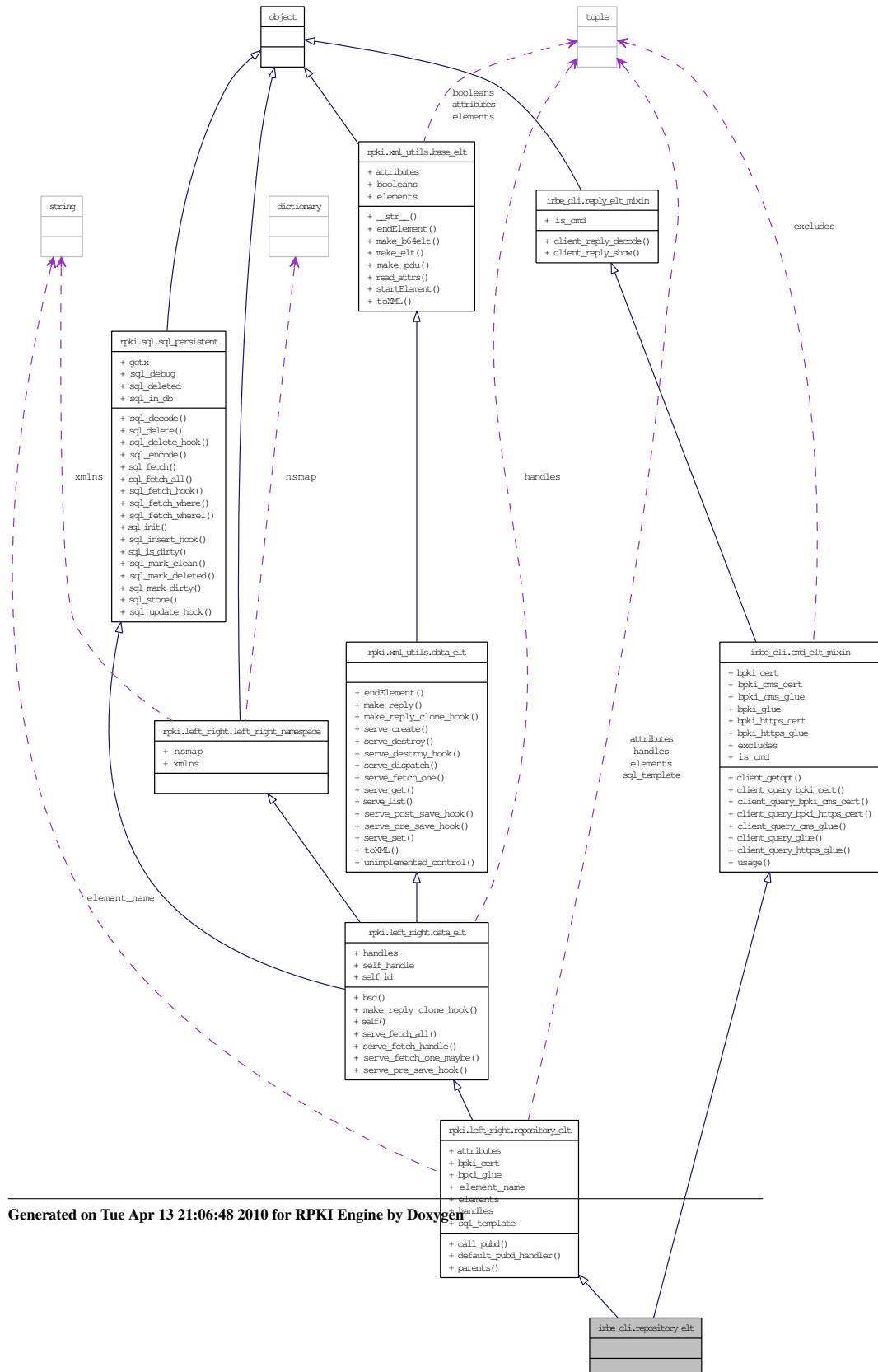
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.27 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:



10.27.1 Detailed Description

Definition at line 177 of file [irbe_cli.py](#).

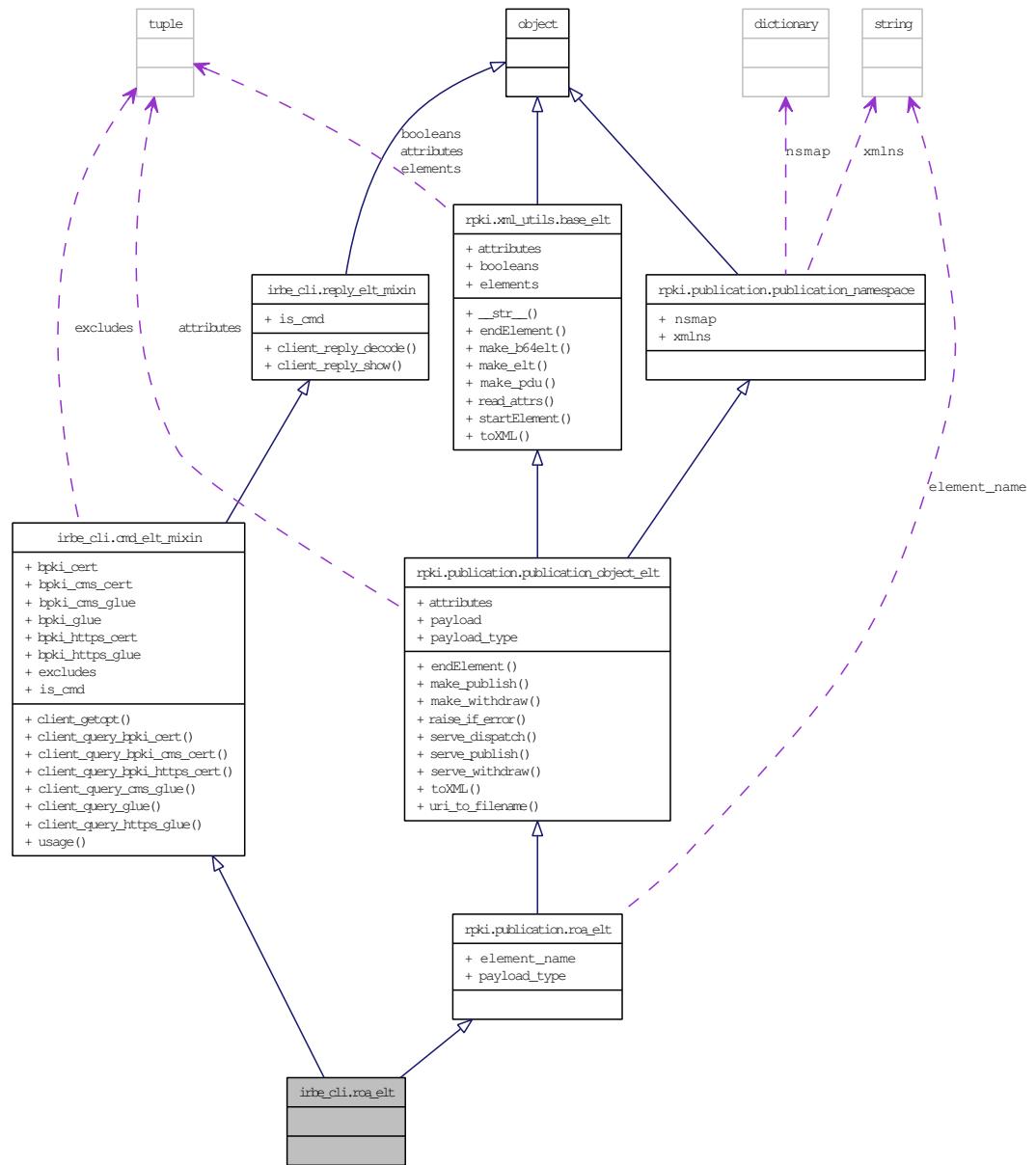
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.28 irbe_cli.roa_elt Class Reference

Inherits [irbe_cli::cmd_elt_mixin](#), and [rpki::publication::roa_elt](#).

Collaboration diagram for irbe_cli.roa_elt:



10.28.1 Detailed Description

Definition at line 220 of file `irbe_cli.py`.

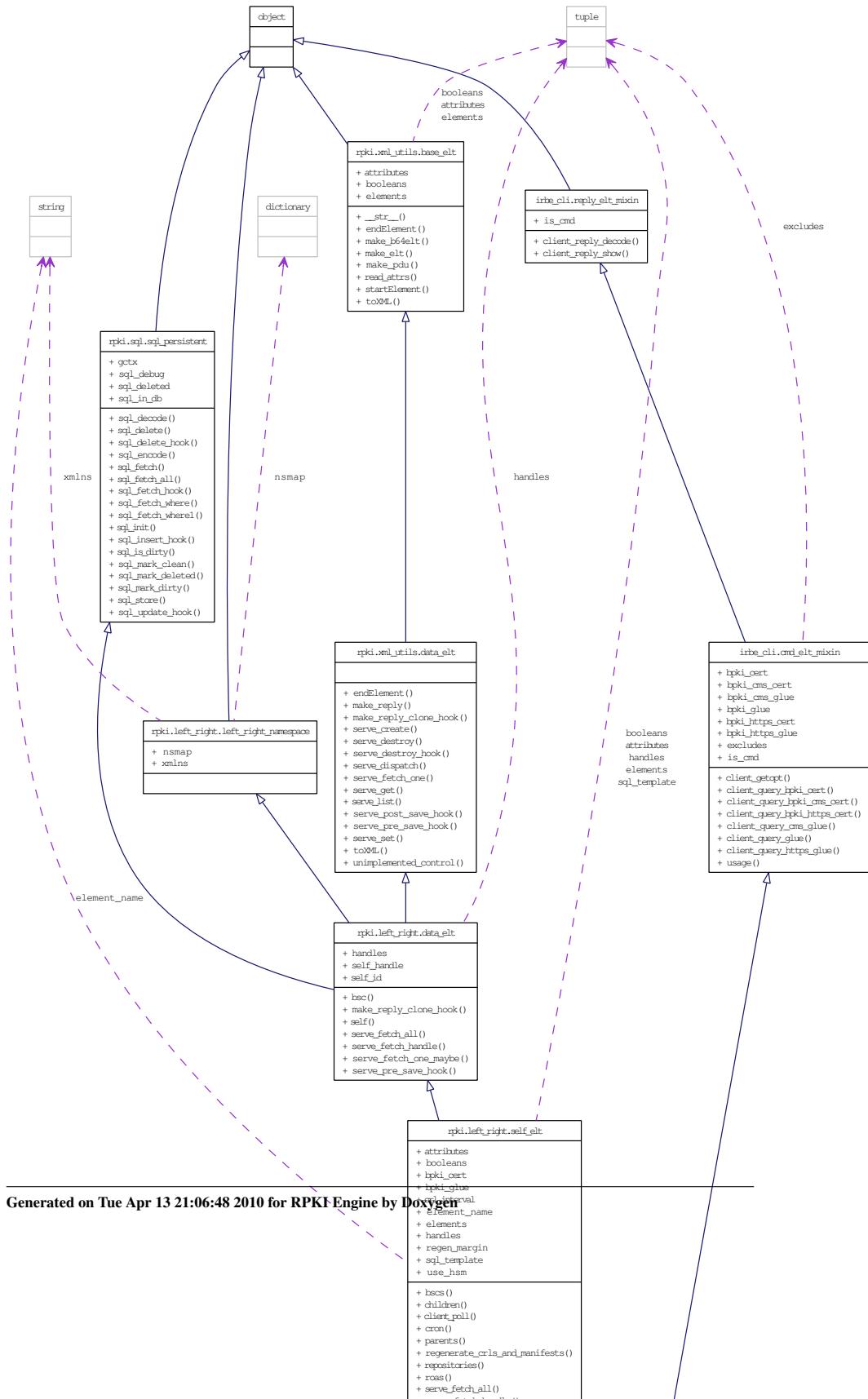
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.29 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:



10.29.1 Detailed Description

Definition at line 149 of file irbe_cli.py.

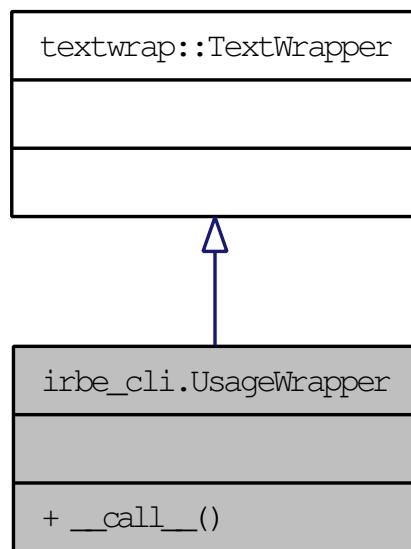
The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.30 irbe_cli.UsageWrapper Class Reference

Inherits [textwrap::TextWrapper](#).

Collaboration diagram for irbe_cli.UsageWrapper:



Public Member Functions

- def [__call__](#)

10.30.1 Detailed Description

Call interface around Python `textwrap.Textwrapper` class.

Definition at line 41 of file irbe_cli.py.

10.30.2 Member Function Documentation

10.30.2.1 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 \(3107\)](#)

10.31 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 \(2424\)](#)

10.32 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.publication.publication_namespace](#), [rpki.resource_set.resource_bag](#), [rpki.resource_set.resource_range](#), [rpki.resource_set.roa_prefix](#), [rpki.rpkid_engine.publication_queue](#), [rpki.rpkid_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](#).

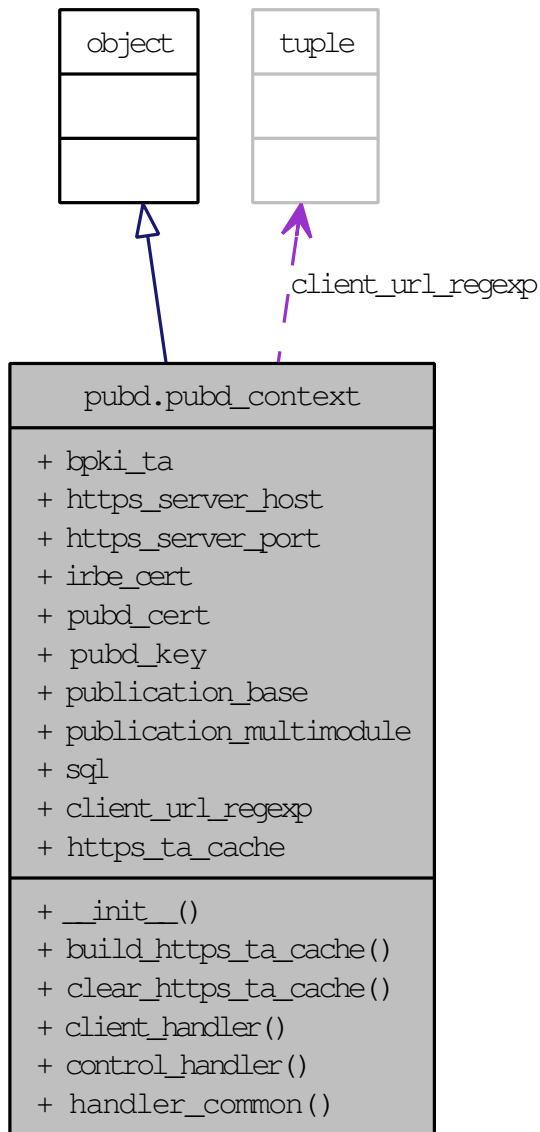
The documentation for this class was generated from the following file:

- [x509.py \(3107\)](#)

10.33 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

- `bpxi_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.

10.33.1 Detailed Description

A container for various pubd parameters.

Definition at line 46 of file pubd.py.

10.33.2 Member Function Documentation

10.33.2.1 def pubd.pubd_context.__init__ (self, cfg)

Definition at line 51 of file pubd.py.

10.33.2.2 def pubd.pubd_context.build_https_ta_cache (self)

Build dynamic TLS trust anchors.

Definition at line 140 of file pubd.py.

10.33.2.3 def pubd.pubd_context.clear_https_ta_cache (*self*)

Clear dynamic TLS trust anchors.

Definition at line 132 of file pubd.py.

10.33.2.4 def pubd.pubd_context.client_handler (*self*, *query*, *path*, *cb*)

Process one PDU from a client.

Definition at line 100 of file pubd.py.

10.33.2.5 def pubd.pubd_context.control_handler (*self*, *query*, *path*, *cb*)

Process one PDU from the IRBE.

Definition at line 80 of file pubd.py.

**10.33.2.6 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.

10.33.3 Member Data Documentation**10.33.3.1 pubd.pubd_context.bpk_i_ta**

Definition at line 55 of file pubd.py.

**10.33.3.2 tuple pubd.pubd_context.client_url_regex =
re.compile("/client/([-A-Z0-9_/.]+)\$", re.I) [static]**

Definition at line 98 of file pubd.py.

10.33.3.3 pubd.pubd_context.https_server_host

Definition at line 60 of file pubd.py.

10.33.3.4 pubd.pubd_context.https_server_port

Definition at line 61 of file pubd.py.

10.33.3.5 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.

10.33.3.6 pubd.pubd_context.irbe_cert

Definition at line 56 of file pubd.py.

10.33.3.7 pubd.pubd_context.pubd_cert

Definition at line 57 of file pubd.py.

10.33.3.8 pubd.pubd_context.pubd_key

Definition at line 58 of file pubd.py.

10.33.3.9 pubd.pubd_context.publication_base

Definition at line 63 of file pubd.py.

10.33.3.10 pubd.pubd_context.publication_multimodule

Definition at line 65 of file pubd.py.

10.33.3.11 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 \(3107\)](#)

10.34 datetime Class Reference

Inherited by [rpki.sundial.datetime](#).

The documentation for this class was generated from the following file:

- [sundial.py \(3191\)](#)

10.35 timedelta Class Reference

Inherited by [rpki.sundial.timedelta](#).

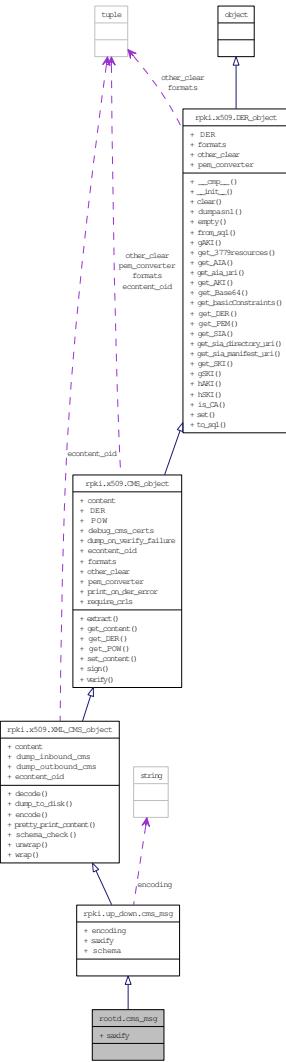
The documentation for this class was generated from the following file:

- [sundial.py \(3191\)](#)

10.36 rootd.cms_msg Class Reference

Inherits [rpki::up_down::cms_msg](#).

Collaboration diagram for rootd.cms_msg:



Static Public Attributes

- `saxify` = `sax_handler.saxify`

10.36.1 Detailed Description

Definition at line 235 of file rootd.py.

10.36.2 Member Data Documentation

10.36.2.1 rootd.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented from [rpki.up_down.cms_msg](#).

Definition at line 236 of file rootd.py.

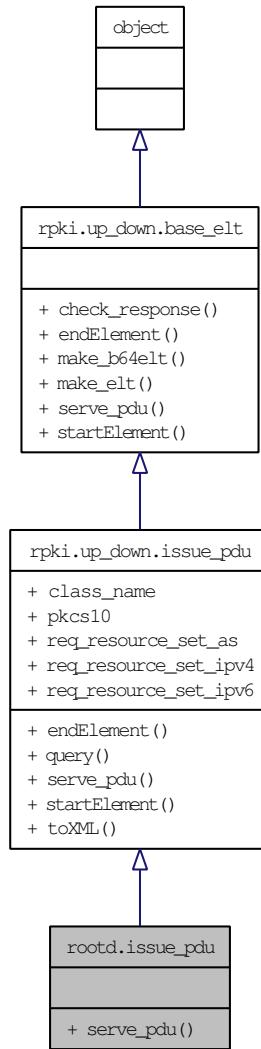
The documentation for this class was generated from the following file:

- [rootd.py \(2913\)](#)

10.37 rootd.issue_pdu Class Reference

Inherits [rpki::up_down::issue_pdu](#).

Collaboration diagram for rootd.issue_pdu:



Public Member Functions

- def [serve_pdu](#)

10.37.1 Detailed Description

Definition at line 194 of file `rootd.py`.

10.37.2 Member Function Documentation

10.37.2.1 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.

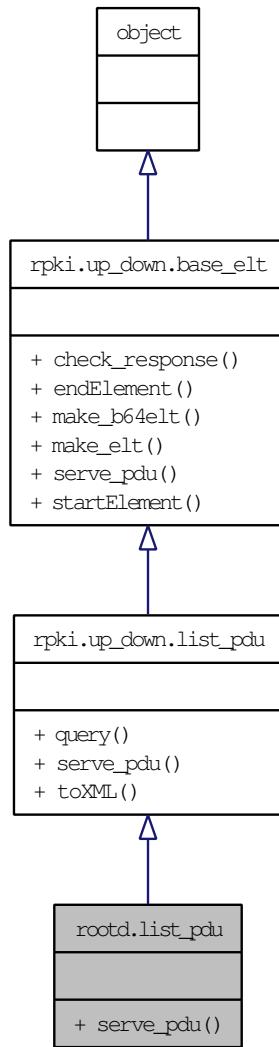
The documentation for this class was generated from the following file:

- [rootd.py \(2913\)](#)

10.38 rootd.list_pdu Class Reference

Inherits [rpki::up_down::list_pdu](#).

Collaboration diagram for rootd.list_pdu:



Public Member Functions

- def [serve_pdu](#)

10.38.1 Detailed Description

Definition at line 188 of file `rootd.py`.

10.38.2 Member Function Documentation

10.38.2.1 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.

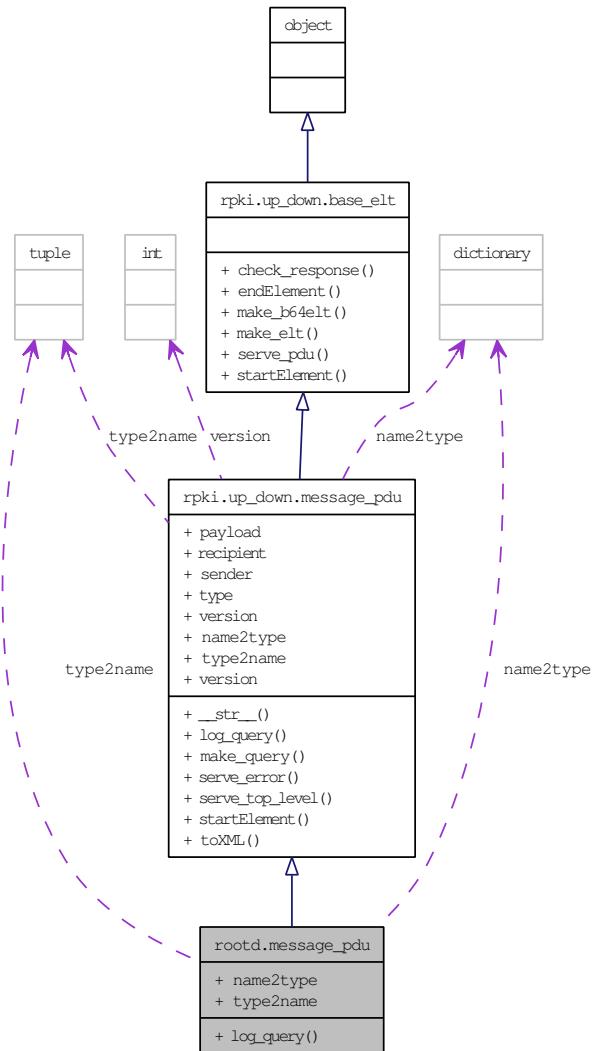
The documentation for this class was generated from the following file:

- [rootd.py \(2913\)](#)

10.39 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())

10.39.1 Detailed Description

Definition at line 213 of file rootd.py.

10.39.2 Member Function Documentation

10.39.2.1 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.

10.39.3 Member Data Documentation

10.39.3.1 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.

10.39.3.2 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.

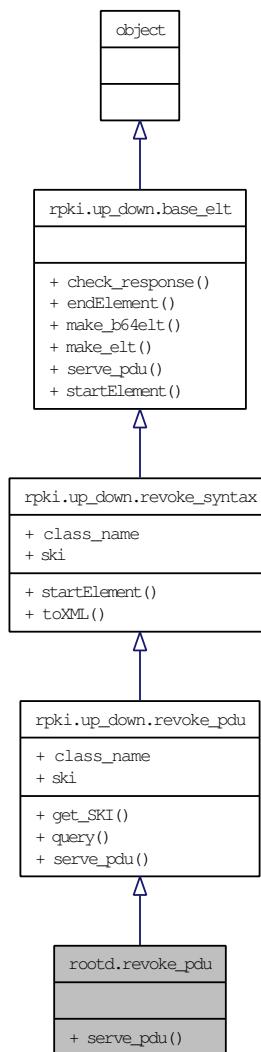
The documentation for this class was generated from the following file:

- [rootd.py \(2913\)](#)

10.40 rootd.revocate_pdu Class Reference

Inherits [rpki::up_down::revocate_pdu](#).

Collaboration diagram for rootd.revocate_pdu:



Public Member Functions

- def [serve_pdu](#)

10.40.1 Detailed Description

Definition at line 201 of file rootd.py.

10.40.2 Member Function Documentation

10.40.2.1 def rootd.revocate_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *cb*, *eb*)

Serve one revoke request PDU.

Reimplemented from [rpki.up_down.revocate_pdu](#).

Definition at line 202 of file rootd.py.

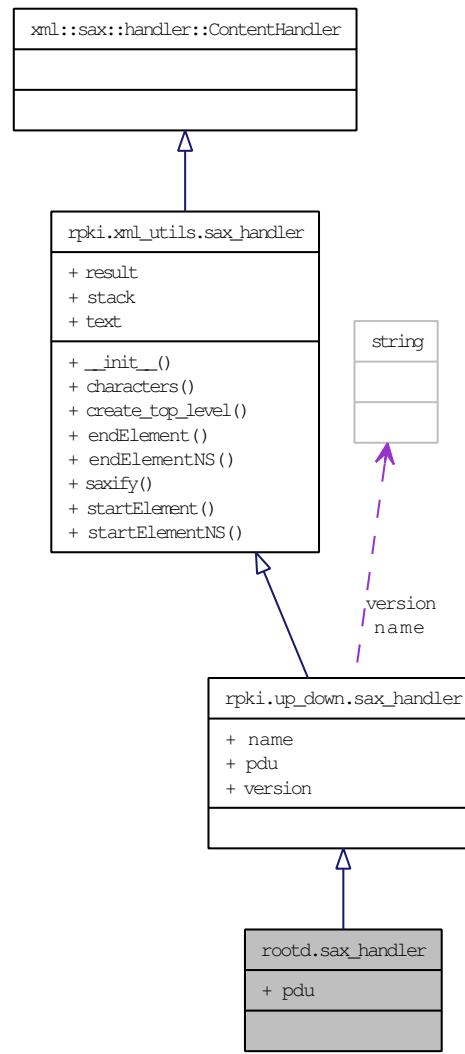
The documentation for this class was generated from the following file:

- [rootd.py \(2913\)](#)

10.41 rootd.sax_handler Class Reference

Inherits [rpki::up_down::sax_handler](#).

Collaboration diagram for rootd.sax_handler:



Static Public Attributes

- `pdu = message_pdu`

10.41.1 Detailed Description

Definition at line 232 of file `rootd.py`.

10.41.2 Member Data Documentation

10.41.2.1 rootd.sax_handler.pdu = message_pdu [static]

Reimplemented from [rpkি.up_down.sax_handler](#).

Definition at line 233 of file rootd.py.

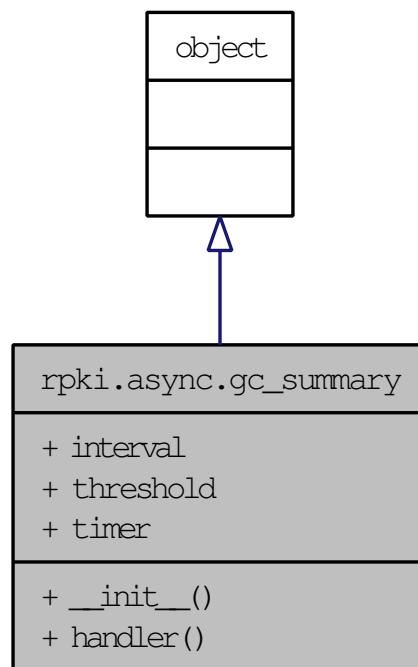
The documentation for this class was generated from the following file:

- [rootd.py \(2913\)](#)

10.42 rpkি.async.gc_summary Class Reference

Inherits [object](#).

Collaboration diagram for rpkি.async.gc_summary:



Public Member Functions

- def [`__init__`](#)

- def [handler](#)

Public Attributes

- [interval](#)
- [threshold](#)
- [timer](#)

10.42.1 Detailed Description

Periodic summary of GC state, for tracking down memory bloat.

Definition at line 368 of file `async.py`.

10.42.2 Member Function Documentation

10.42.2.1 def rpkি.async.gc_summary.__init__ (*self*, *interval*, *threshold* = 0)

Definition at line 373 of file `async.py`.

10.42.2.2 def rpkি.async.gc_summary.handler (*self*)

Collect and log GC state for this period, reset timer.

Definition at line 381 of file `async.py`.

10.42.3 Member Data Documentation

10.42.3.1 rpkি.async.gc_summary.interval

Definition at line 376 of file `async.py`.

10.42.3.2 rpkি.async.gc_summary.threshold

Definition at line 377 of file `async.py`.

10.42.3.3 rpki.async.gc_summary.timer

Definition at line 378 of file `async.py`.

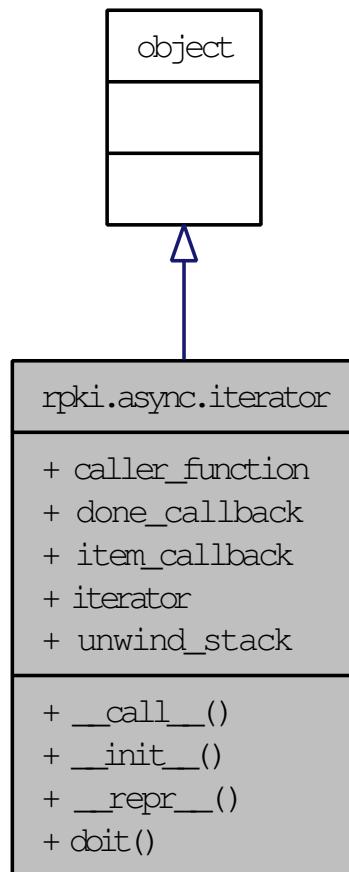
The documentation for this class was generated from the following file:

- [async.py \(3191\)](#)

10.43 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](#)

10.43.1 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`.

10.43.2 Member Function Documentation

10.43.2.1 def rpki.async.iterator.[__call__](#) (*self*)

Definition at line 64 of file `async.py`.

**10.43.2.2 def rpki.async.iterator.__init__ (*self*, *iterable*, *item_callback*,
done_callback, *unwind_stack* = **True**)**

Definition at line 45 of file async.py.

10.43.2.3 def rpki.async.iterator.__repr__ (*self*)

Definition at line 59 of file async.py.

10.43.2.4 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.

10.43.3 Member Data Documentation**10.43.3.1 rpki.async.iterator.caller_function**

Definition at line 48 of file async.py.

10.43.3.2 rpki.async.iterator.done_callback

Definition at line 47 of file async.py.

10.43.3.3 rpki.async.iterator.item_callback

Definition at line 46 of file async.py.

10.43.3.4 rpki.async.iterator.iterator

Definition at line 51 of file `async.py`.

10.43.3.5 rpki.async.iterator.unwind_stack

Definition at line 49 of file `async.py`.

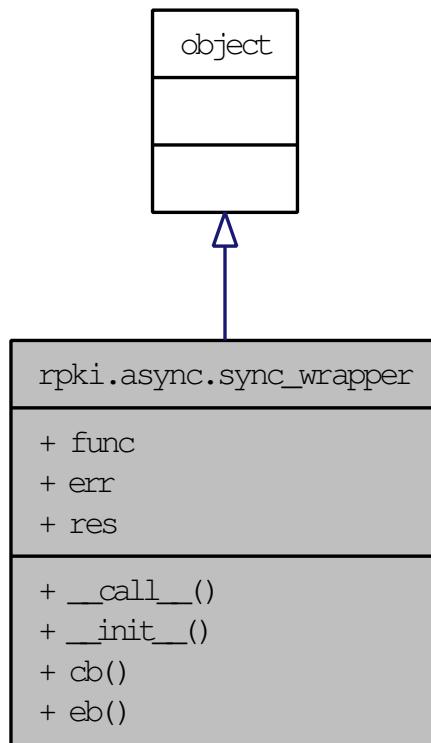
The documentation for this class was generated from the following file:

- [async.py \(3191\)](#)

10.44 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`

10.44.1 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.

10.44.2 Member Function Documentation

10.44.2.1 def rpki.async.sync_wrapper.__call__ (*self*, *args*, *kwargs*)

Definition at line 340 of file async.py.

10.44.2.2 def rpki.async.sync_wrapper.__init__ (*self*, *func*)

Definition at line 320 of file async.py.

10.44.2.3 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.

10.44.2.4 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.

10.44.3 Member Data Documentation**10.44.3.1 rpki.async.sync_wrapper.err = None [static]**

Definition at line 318 of file `async.py`.

10.44.3.2 rpki.async.sync_wrapper.func

Definition at line 321 of file `async.py`.

10.44.3.3 rpki.async.sync_wrapper.res = None [static]

Definition at line 317 of file `async.py`.

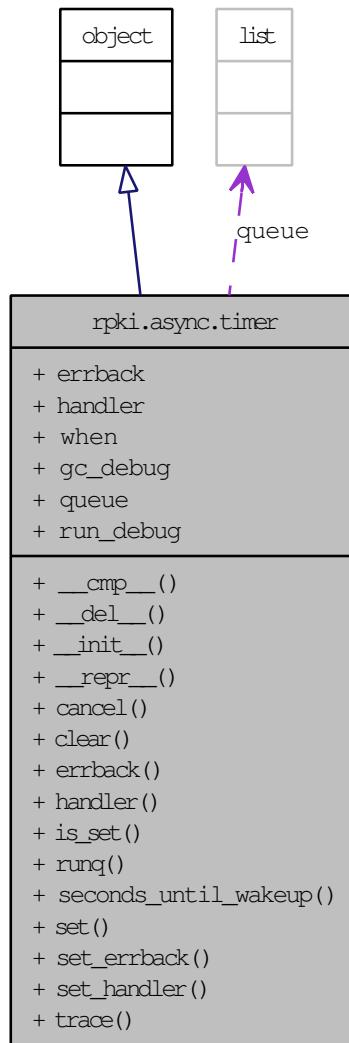
The documentation for this class was generated from the following file:

- [async.py \(3191\)](#)

10.45 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.

10.45.1 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 wakeup 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 explicit handler turns out to be very convenient when combined with bound methods to other objects.

Definition at line 82 of file `async.py`.

10.45.2 Member Function Documentation

10.45.2.1 def rpki.async.timer.__cmp__ (*self, other*)

Definition at line 142 of file async.py.

10.45.2.2 def rpki.async.timer.__del__ (*self*)

Definition at line 146 of file async.py.

10.45.2.3 def rpki.async.timer.__init__ (*self, handler = None, errback = None*)

Definition at line 109 of file async.py.

10.45.2.4 def rpki.async.timer.__repr__ (*self*)

Definition at line 209 of file async.py.

10.45.2.5 def rpki.async.timer.cancel (*self*)

Cancel a timer, if it was set.

Definition at line 149 of file async.py.

10.45.2.6 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.

10.45.2.7 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`.

10.45.2.8 def rpki.async.timer.handler (*self*)

Handle a timer that has expired. This must either be overridden by a subclass or set dynamically by `set_handler()`.

Definition at line 164 of file `async.py`.

10.45.2.9 def rpki.async.timer.is_set (*self*)

Test whether this timer is currently set.

Definition at line 160 of file `async.py`.

10.45.2.10 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`.

10.45.2.11 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`.

10.45.2.12 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.

10.45.2.13 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.

10.45.2.14 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.

10.45.2.15 def rpki.async.timer.trace (*self*, *msg*)

Debug logging.

Definition at line 118 of file async.py.

10.45.3 Member Data Documentation**10.45.3.1 rpki.async.timer.errback**

Definition at line 190 of file async.py.

10.45.3.2 rpkic::async.timer::gc_debug = False [static]

Verbose chatter about timers states and garbage collection.

Definition at line 99 of file `async.py`.

10.45.3.3 rpkic.async.timer.handler

Definition at line 179 of file `async.py`.

10.45.3.4 rpkic::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`.

10.45.3.5 rpkic::async.timer::run_debug = False [static]

Verbose chatter about timers being run.

Definition at line 103 of file `async.py`.

10.45.3.6 rpkic.async.timer.when

Definition at line 114 of file `async.py`.

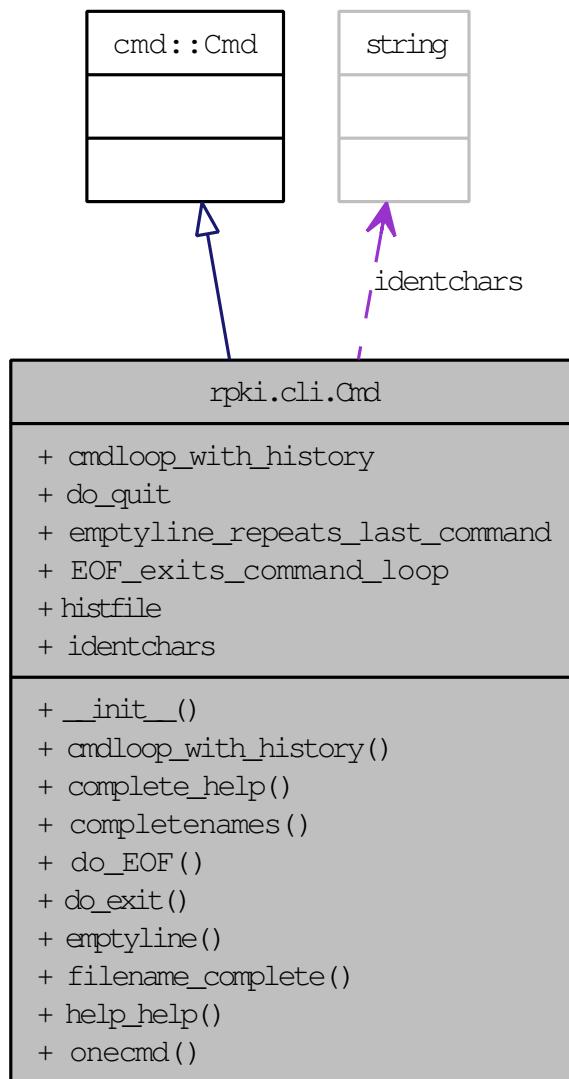
The documentation for this class was generated from the following file:

- [async.py \(3191\)](#)

10.46 rpkicli.Cmd Class Reference

Inherits [cmd::Cmd](#).

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` = "/-."

10.46.1 Detailed Description

Customized subclass of Python cmd module.

Definition at line 29 of file cli.py.

10.46.2 Member Function Documentation

10.46.2.1 def rpki.cli.Cmd.__init__ (*self*, *argv* = **None**)

Definition at line 42 of file cli.py.

10.46.2.2 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.

10.46.2.3 def rpki.cli.Cmd.complete_help (*self*, *args*)

Better completion function for help command arguments.

Definition at line 119 of file cli.py.

10.46.2.4 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.

10.46.2.5 def rpki.cli.Cmd.do_EOF (*self*, *arg*)

Exit program.

Definition at line 61 of file cli.py.

10.46.2.6 def rpki.cli.Cmd.do_exit (*self*, *arg*)

Exit program.

Definition at line 69 of file cli.py.

10.46.2.7 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 principle of least astonishment, so my preference is that an empty line does nothing.

Definition at line 77 of file cli.py.

10.46.2.8 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.

10.46.2.9 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.

10.46.2.10 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.

10.46.3 Member Data Documentation**10.46.3.1 rpki.cli.Cmd.cmdloop_with_history = cmd.Cmd.cmdloop
[static]**

Definition at line 153 of file cli.py.

10.46.3.2 rpki.cli.Cmd.do_quit = do_exit [static]

Definition at line 75 of file cli.py.

10.46.3.3 rpki.cli.Cmd.emptyline_repeats_last_command = False [static]

Definition at line 34 of file cli.py.

10.46.3.4 rpki.cli.Cmd.EOF_exits_command_loop = True [static]

Definition at line 36 of file cli.py.

10.46.3.5 rpki.cli.Cmd.histfile = None [static]

Definition at line 40 of file cli.py.

10.46.3.6 string rpki.cli.Cmd.identchars = "/-." [static]

Definition at line 38 of file cli.py.

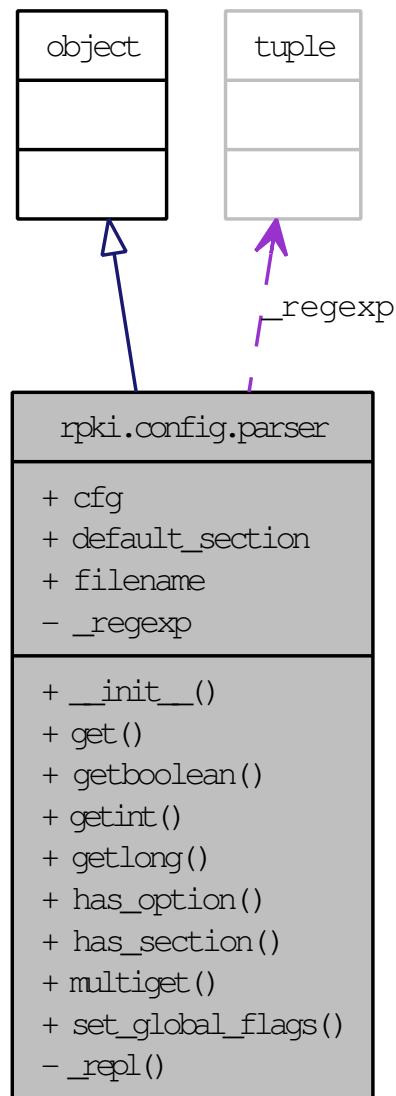
The documentation for this class was generated from the following file:

- [cli.py \(3191\)](#)

10.47 rpki.config.parser Class Reference

Inherits [object](#).

Collaboration diagram for rpkiconfig.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("``\\${(.*)?::(.*)?}``")

10.47.1 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.

10.47.2 Member Function Documentation

10.47.2.1 def rpki.config.parser.`__init__` (`self, filename, section = None, allow_missing = False`)

Initialize this parser.

Definition at line 50 of file config.py.

10.47.2.2 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.

10.47.2.3 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.

10.47.2.4 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.

10.47.2.5 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.

10.47.2.6 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.

10.47.2.7 def rpki.config.parser.has_option (*self*, *option*, *section* = **None)**

Test whether an option exists.

Definition at line 71 of file config.py.

10.47.2.8 def rpki.config.parser.has_section (*self*, *section*)

Test whether a section exists.

Definition at line 64 of file config.py.

10.47.2.9 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.

10.47.2.10 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.

10.47.3 Member Data Documentation**10.47.3.1 tuple rpki.config.parser._regexp = re.compile("\\\\${(.*)::(.*)}")
[static, private]**

Definition at line 99 of file config.py.

10.47.3.2 rpki.config.parser.cfg

Definition at line 56 of file config.py.

10.47.3.3 rpki.config.parser.default_section

Definition at line 62 of file config.py.

10.47.3.4 rpki.config.parser.filename

Definition at line 55 of file config.py.

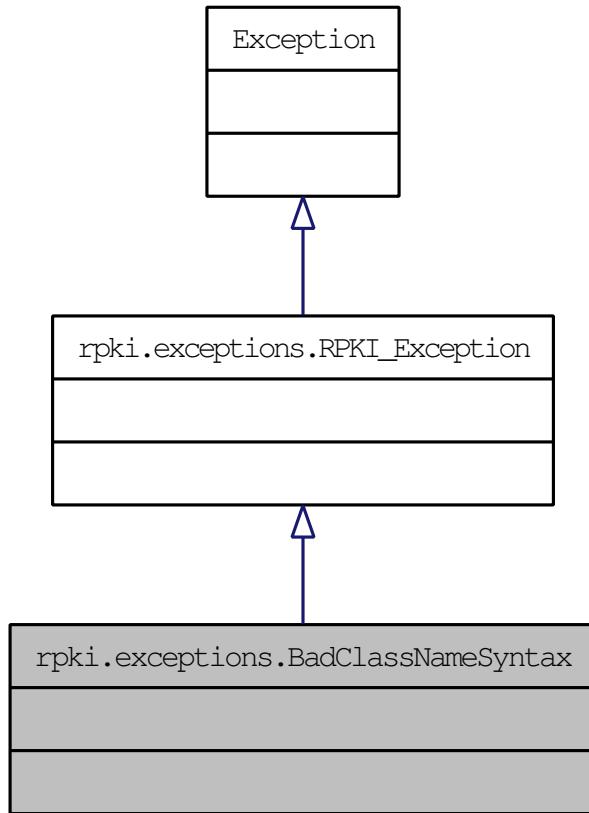
The documentation for this class was generated from the following file:

- [config.py \(3107\)](#)

10.48 rpki.exceptions.BadClassNameSyntax Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.BadClassNameSyntax:



10.48.1 Detailed Description

Illegal syntax for a class_name.

Definition at line 92 of file exceptions.py.

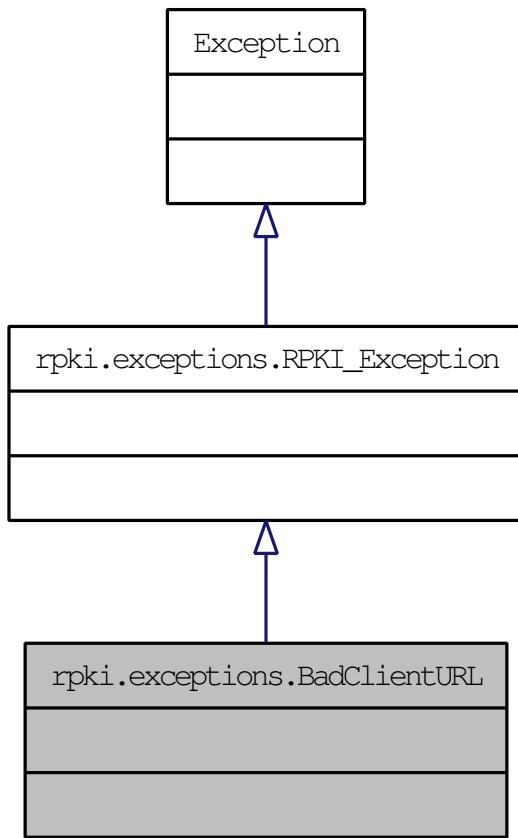
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.49 rpki.exceptions.BadClientURL Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.BadClientURL:



10.49.1 Detailed Description

URL given to HTTPS client does not match profile.

Definition at line 232 of file exceptions.py.

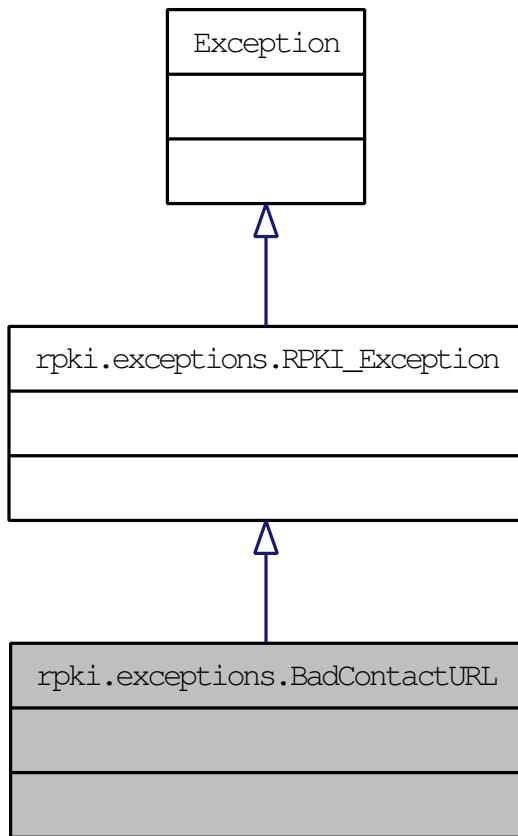
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.50 rpki.exceptions.BadContactURL Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.BadContactURL:



10.50.1 Detailed Description

Error trying to parse contact URL.

Definition at line 87 of file `exceptions.py`.

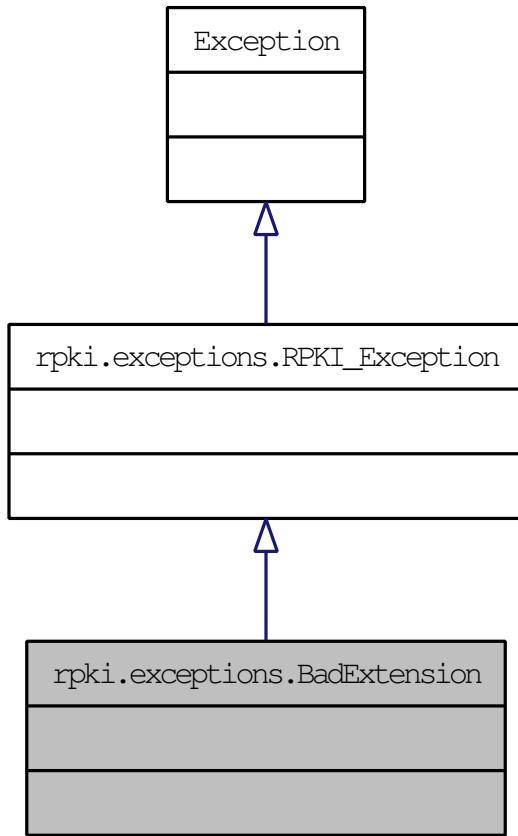
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.51 rpki.exceptions.BadExtension Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.BadExtension:



10.51.1 Detailed Description

Forbidden X.509 extension.

Definition at line 242 of file exceptions.py.

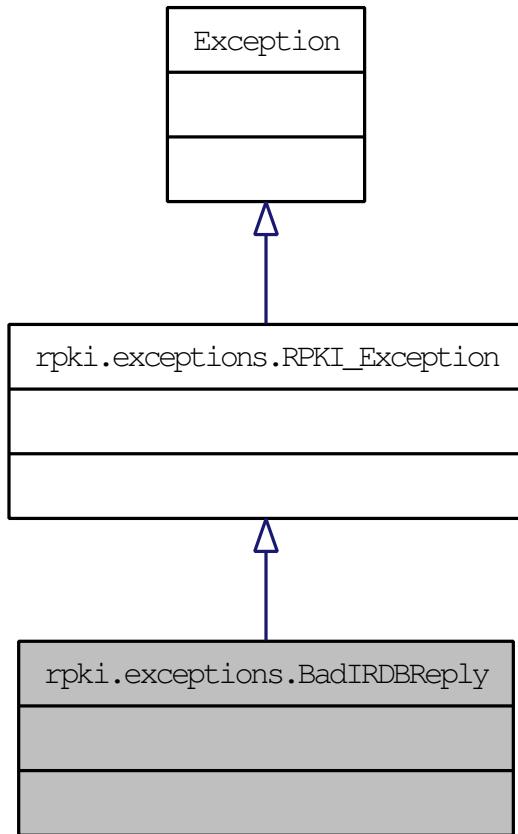
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.52 rpki.exceptions.BadIRDBReply Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.BadIRDBReply:



10.52.1 Detailed Description

Unexpected reply to IRDB query.

Definition at line 152 of file exceptions.py.

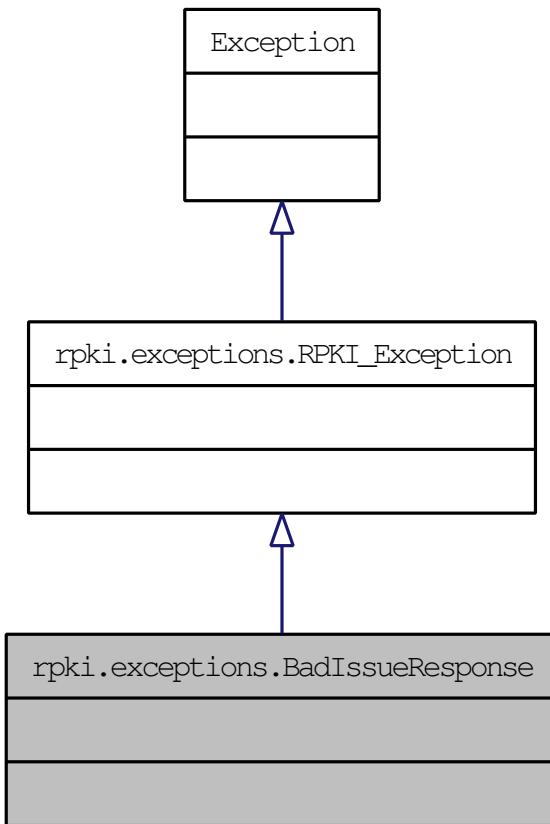
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.53 rpki.exceptions.BadIssueResponse Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpkி.exceptions.BadIssueResponse:



10.53.1 Detailed Description

issue_response PDU with wrong number of classes or certificates.

Definition at line 97 of file exceptions.py.

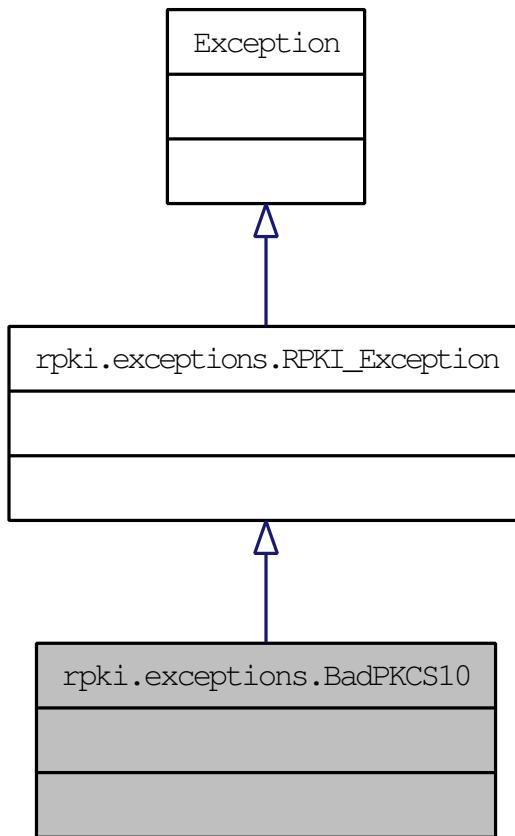
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.54 rpkி.exceptions.BadPKCS10 Class Reference

Inherits [rpkி.exceptions.RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.BadPKCS10:



10.54.1 Detailed Description

Bad PKCS #10 object.

Definition at line 107 of file `exceptions.py`.

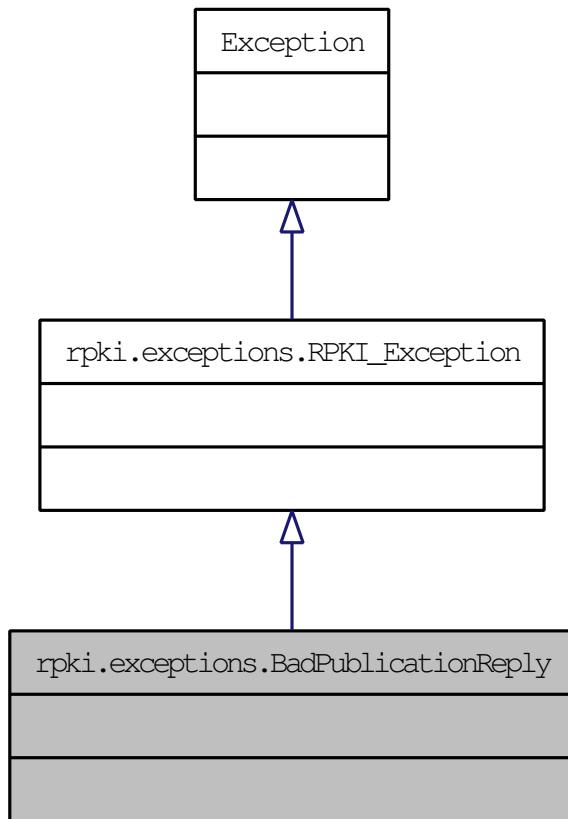
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.55 rpki.exceptions.BadPublicationReply Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpkி.exceptions.BadPublicationReply:



10.55.1 Detailed Description

Unexpected reply to publication query.

Definition at line 257 of file exceptions.py.

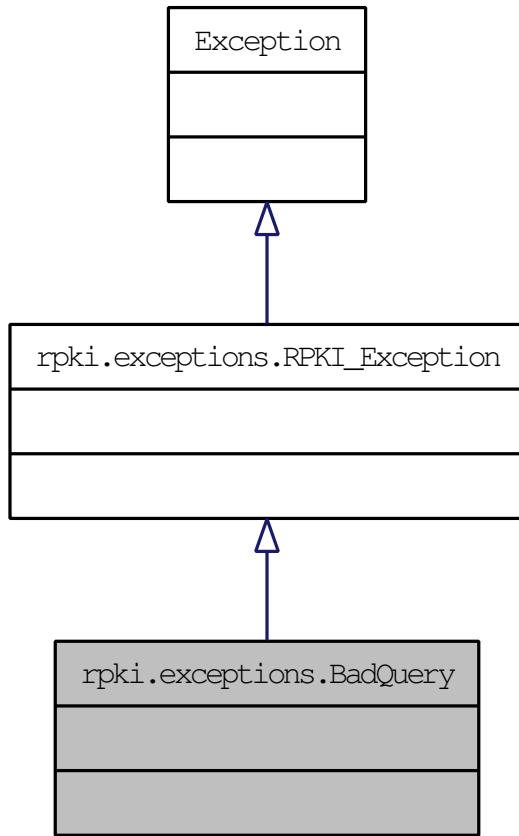
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.56 rpkி.exceptions.BadQuery Class Reference

Inherits [rpkி.exceptions.RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.BadQuery:



10.56.1 Detailed Description

Unexpected protocol query.

Definition at line 55 of file exceptions.py.

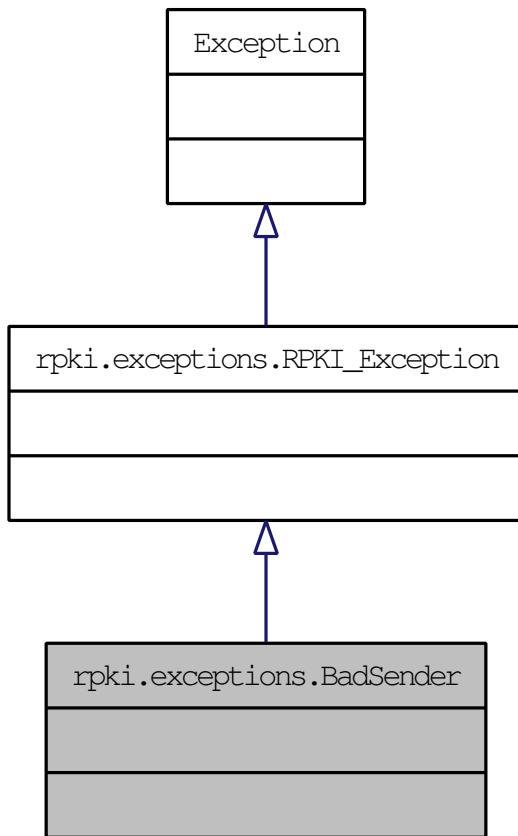
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.57 rpki.exceptions.BadSender Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.BadSender:



10.57.1 Detailed Description

Unexpected XML sender value.

Definition at line 127 of file exceptions.py.

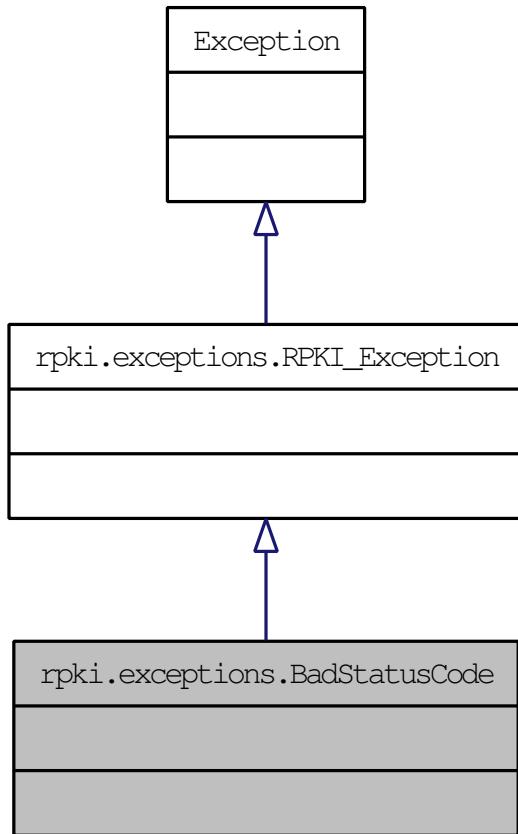
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.58 rpki.exceptions.BadStatusCode Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.BadStatusCode:



10.58.1 Detailed Description

Unrecognized protocol status code.

Definition at line 50 of file `exceptions.py`.

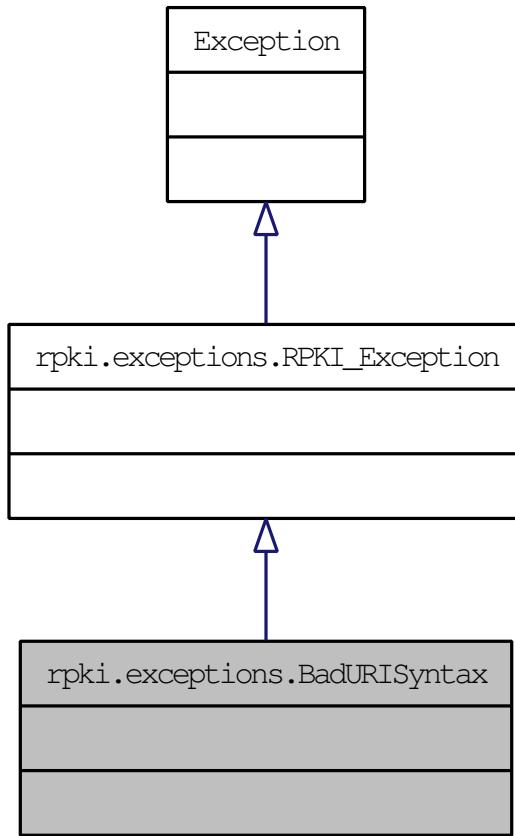
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.59 rpki.exceptions.BadURISyntax Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.BadURISyntax:



10.59.1 Detailed Description

Illegal syntax for a URI.

Definition at line 45 of file exceptions.py.

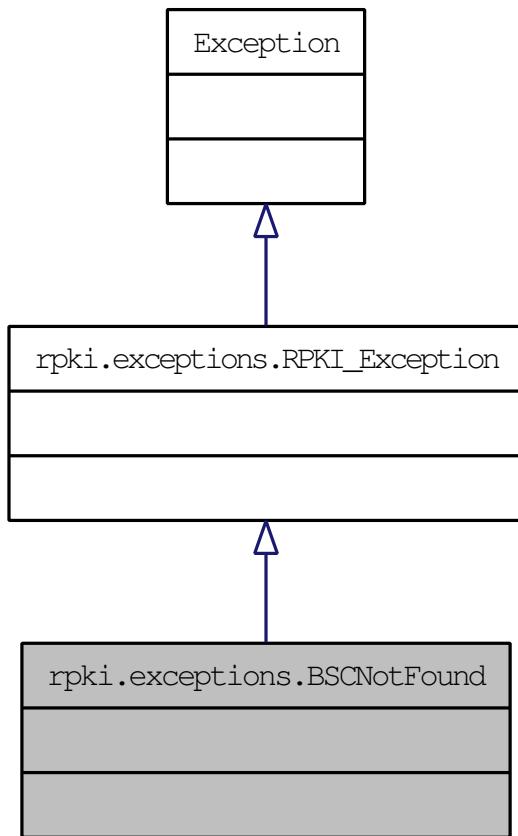
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.60 rpki.exceptions.BSCNotFound Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.BSCNotFound:



10.60.1 Detailed Description

Could not find specified BSC in database.

Definition at line 122 of file exceptions.py.

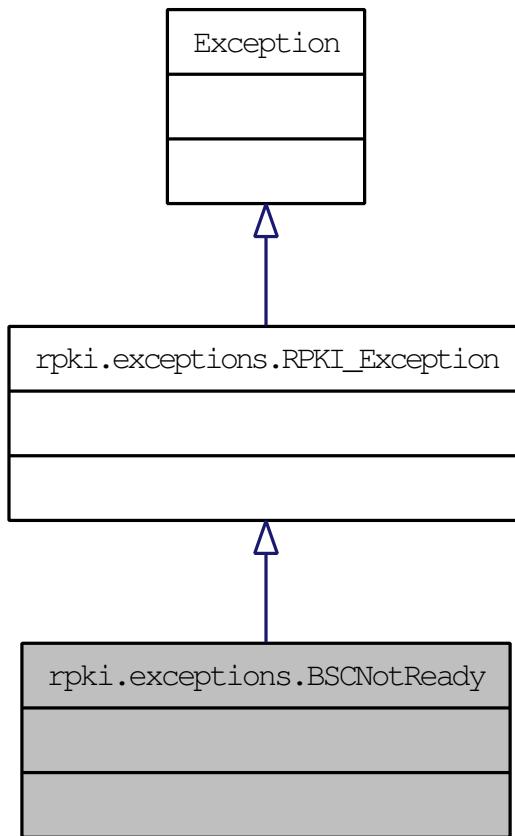
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.61 rpki.exceptions.BSCNotReady Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.BSCNotReady:



10.61.1 Detailed Description

BSC not yet in a usable state, `signing_cert` not set.

Definition at line 277 of file `exceptions.py`.

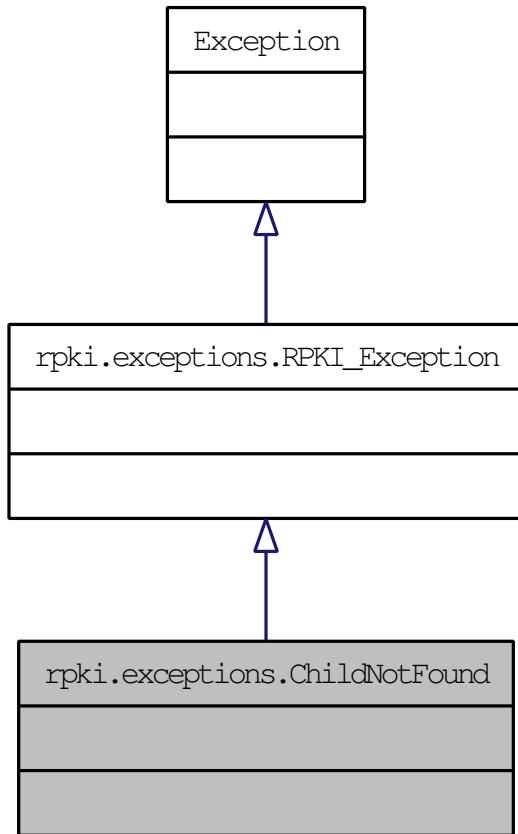
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.62 rpki.exceptions.ChildNotFound Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.ChildNotFound:



10.62.1 Detailed Description

Could not find specified child in database.

Definition at line 117 of file `exceptions.py`.

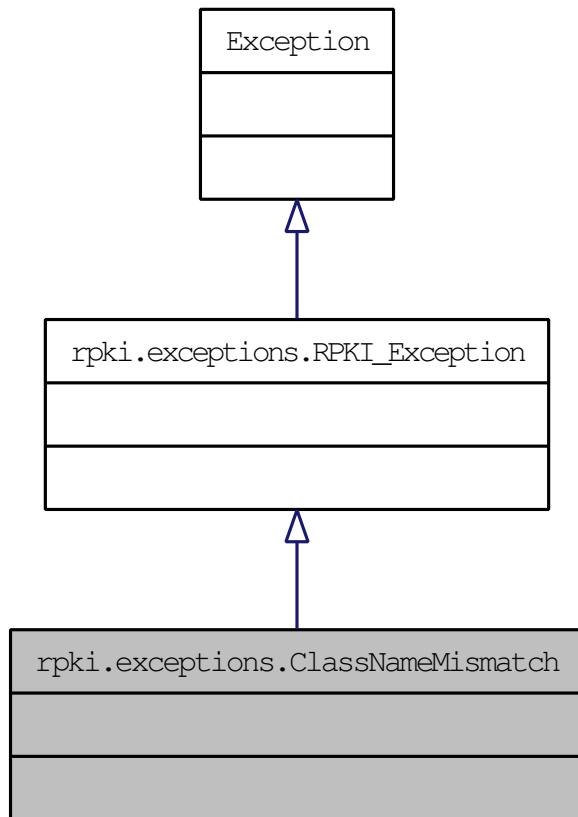
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.63 rpki.exceptions.ClassNameMismatch Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.ClassNameMismatch:



10.63.1 Detailed Description

`class_name` does not match child context.

Definition at line 132 of file `exceptions.py`.

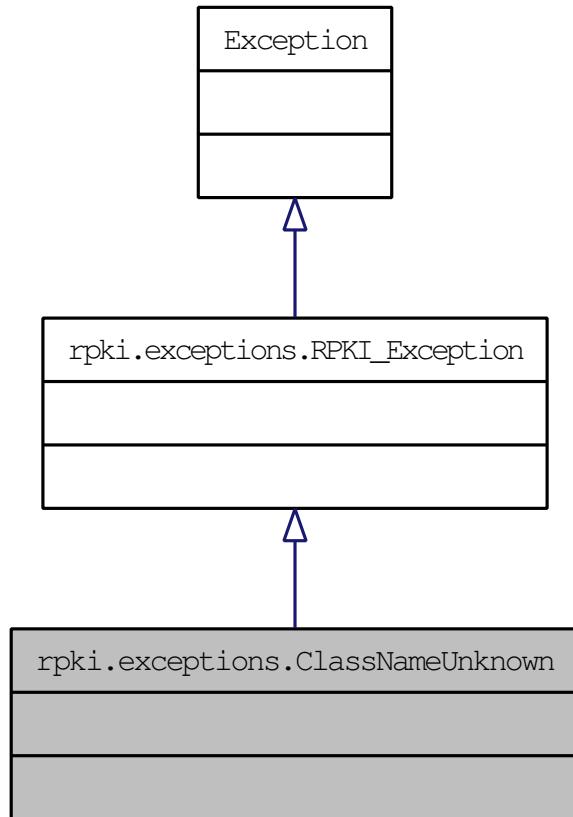
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.64 rpki.exceptions.ClassNameUnknown Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpkி.exceptions.ClassNameUnknown:



10.64.1 Detailed Description

Unknown class_name.

Definition at line 137 of file exceptions.py.

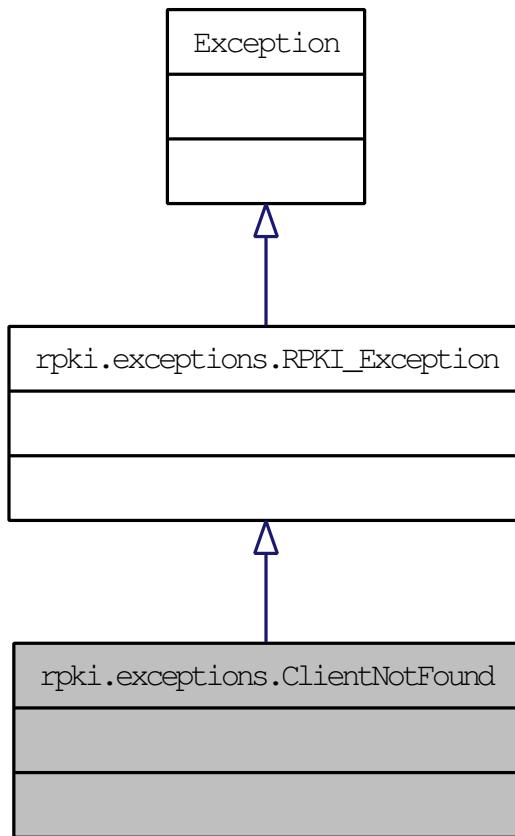
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.65 rpkி.exceptions.ClientNotFound Class Reference

Inherits [rpkième.exceptions.RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.ClientNotFound:



10.65.1 Detailed Description

Could not find specified client in database.

Definition at line 237 of file exceptions.py.

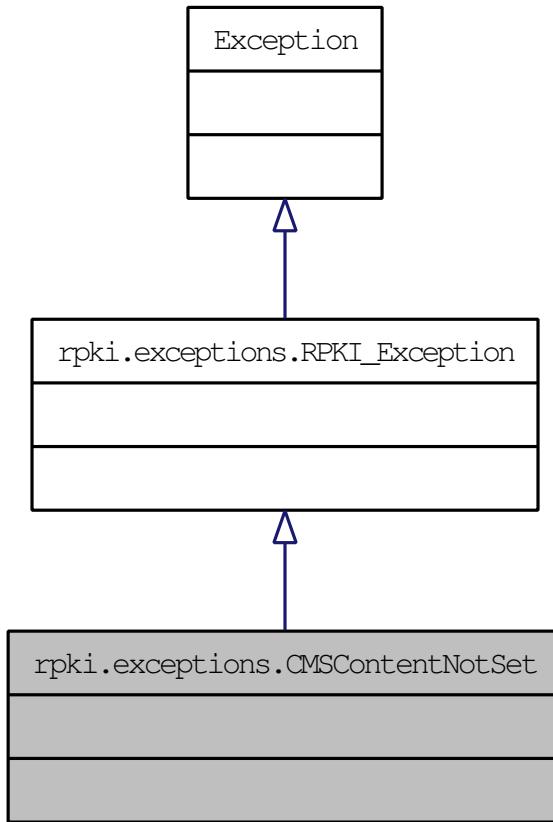
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.66 rpki.exceptions.CMSContentNotSet Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpkி.exceptions.CMSContentNotSet:



10.66.1 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.

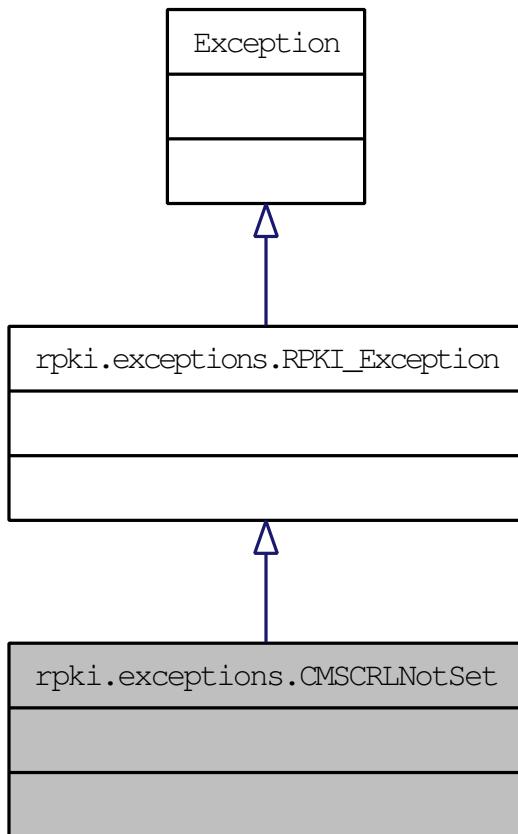
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.67 rpkி.exceptions.CMSCRLNotSet Class Reference

Inherits [rpkி::exceptions::RPKI_Exception](#).

Collaboration diagram for rpkி.exceptions.CMSCRLNotSet:



10.67.1 Detailed Description

CMS CRL has not been configured.

Definition at line 217 of file exceptions.py.

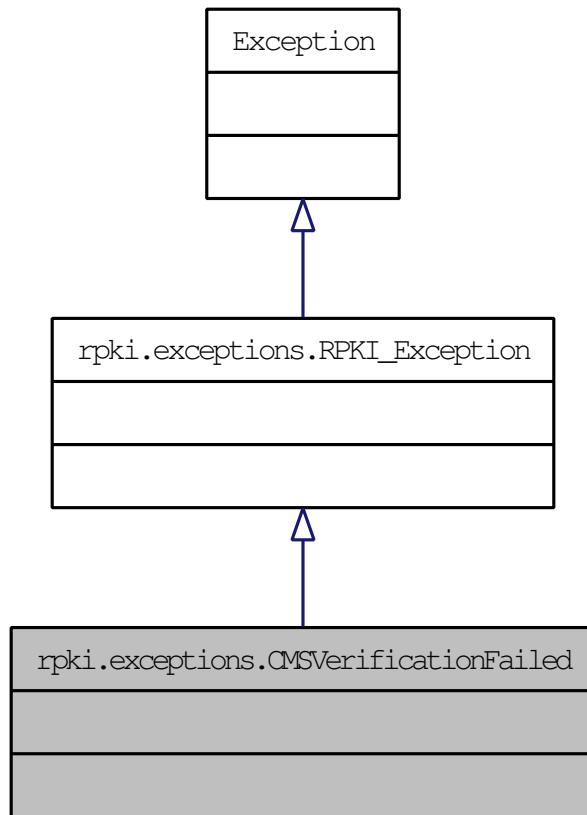
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.68 rpki.exceptions.CMSVerificationFailed Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.CMSVerificationFailed:



10.68.1 Detailed Description

Verification of a CMS message failed.

Definition at line 66 of file `exceptions.py`.

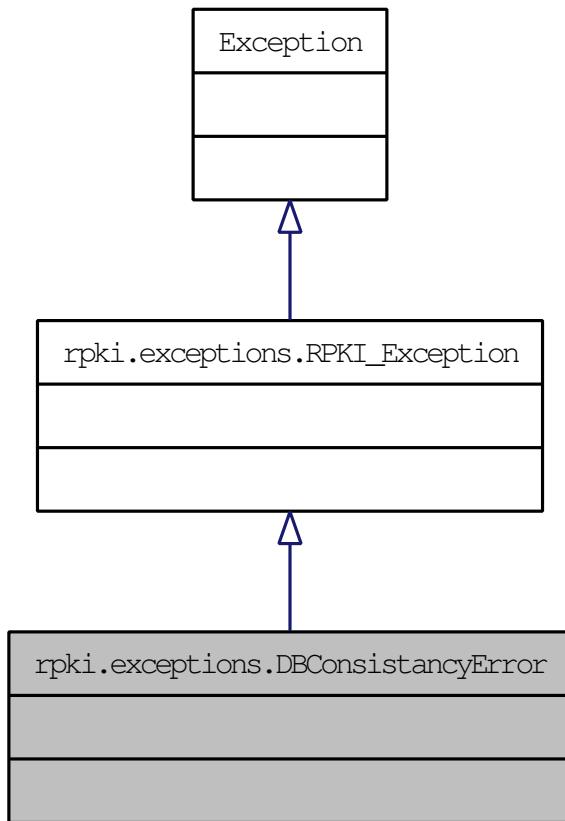
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.69 rpki.exceptions.DBConsistencyError Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.DBConsistencyError:



10.69.1 Detailed Description

Found multiple matches for a database query that shouldn't ever return that.

Definition at line 60 of file exceptions.py.

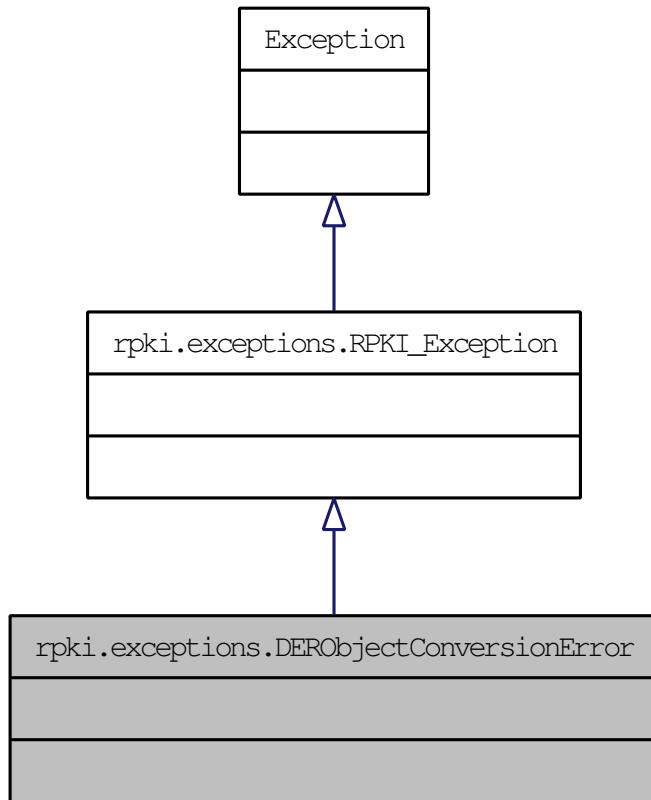
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.70 rpkி.exceptions.DERObjectConversionError Class Reference

Inherits [rpkி::exceptions::RPKI_Exception](#).

Collaboration diagram for rpkி.exceptions.DERObjectConversionError:



10.70.1 Detailed Description

Error trying to convert a DER-based object from one representation to another.

Definition at line 76 of file exceptions.py.

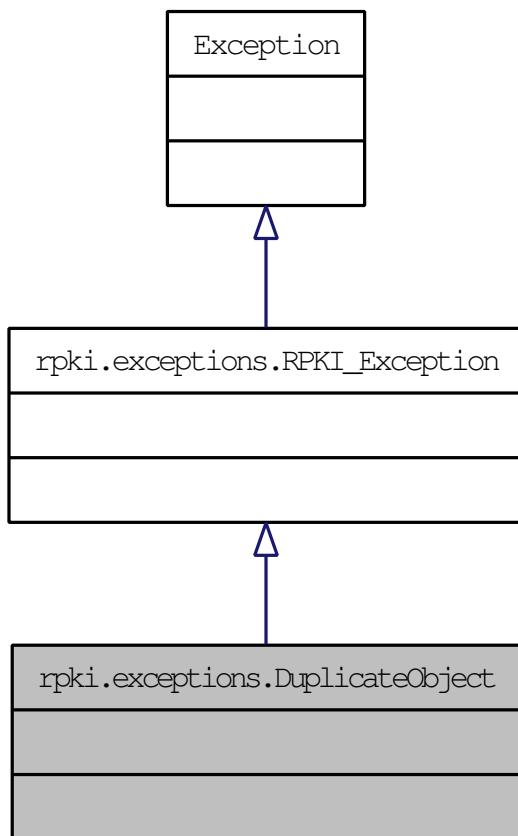
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.71 rpki.exceptions.DuplicateObject Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.DuplicateObject:



10.71.1 Detailed Description

Attempt to create an object that already exists.

Definition at line 262 of file exceptions.py.

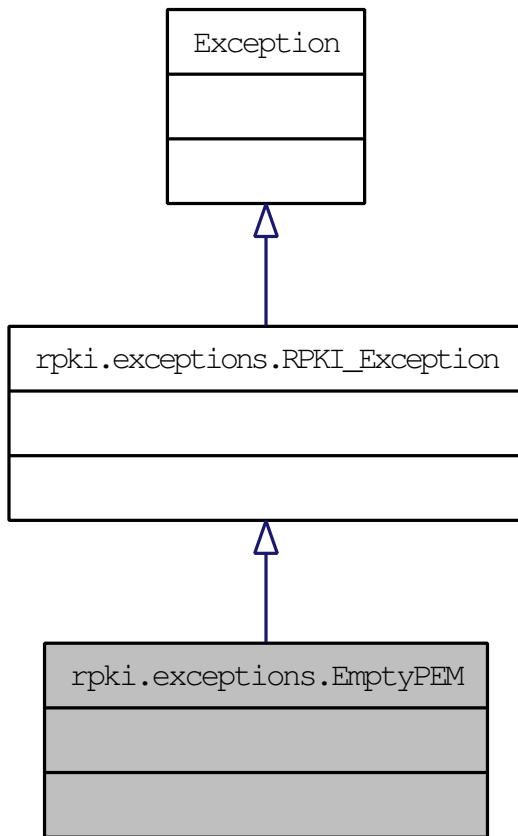
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.72 rpki.exceptions.EmptyPEM Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.EmptyPEM:



10.72.1 Detailed Description

Couldn't find PEM block to convert.

Definition at line 187 of file `exceptions.py`.

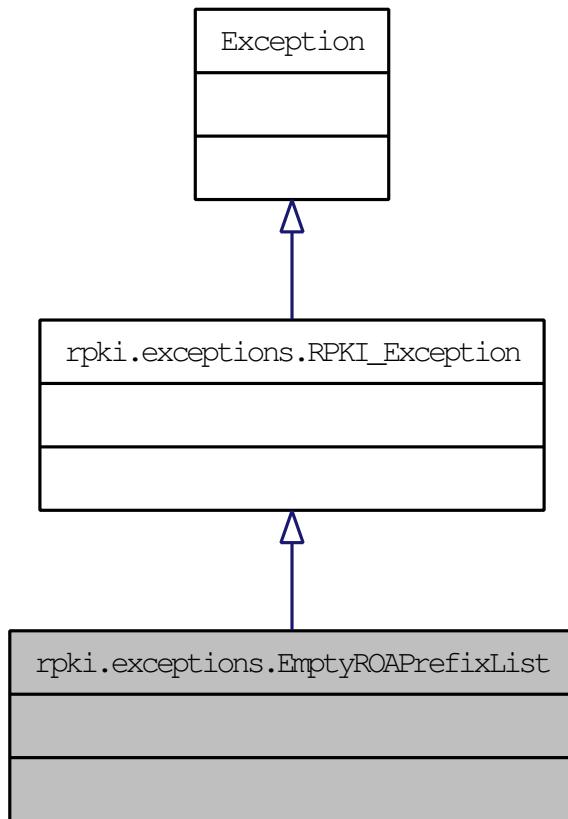
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.73 rpki.exceptions.EmptyROAPrefixList Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.EmptyROAPrefixList:



10.73.1 Detailed Description

Can't create ROA with an empty prefix list.

Definition at line 267 of file `exceptions.py`.

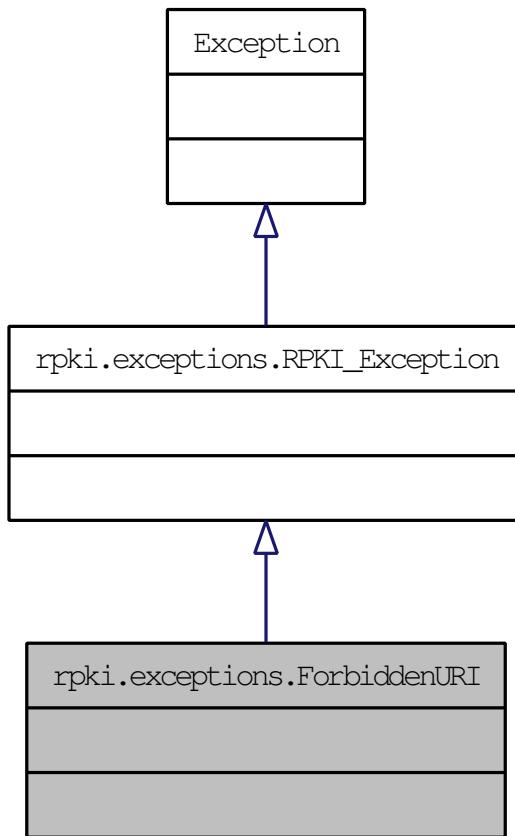
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.74 rpki.exceptions.ForbiddenURI Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.ForbiddenURI:



10.74.1 Detailed Description

Forbidden URI, does not start with correct base URI.

Definition at line 247 of file exceptions.py.

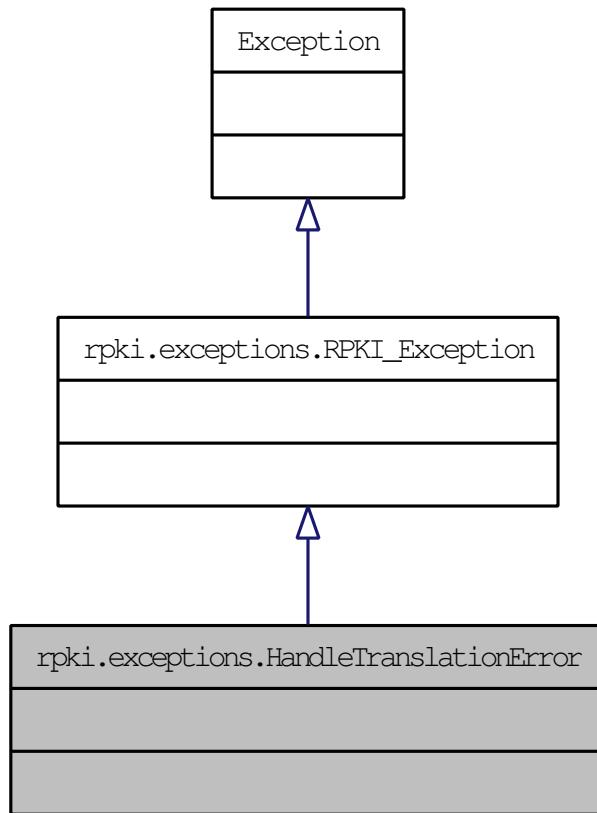
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.75 rpki.exceptions.HandleTranslationError Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.HandleTranslationError:



10.75.1 Detailed Description

Internal error translating protocol handle -> SQL id.

Definition at line 292 of file `exceptions.py`.

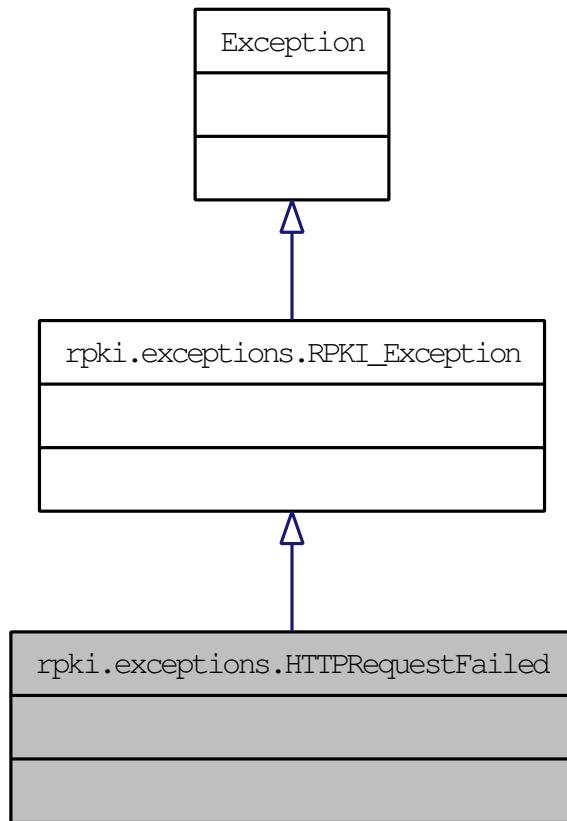
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.76 rpkி.exceptions.HTTPRequestFailed Class Reference

Inherits [rpkி::exceptions::RPKI_Exception](#).

Collaboration diagram for rpkி.exceptions.HTTPRequestFailed:



10.76.1 Detailed Description

HTTP request failed.

Definition at line 71 of file exceptions.py.

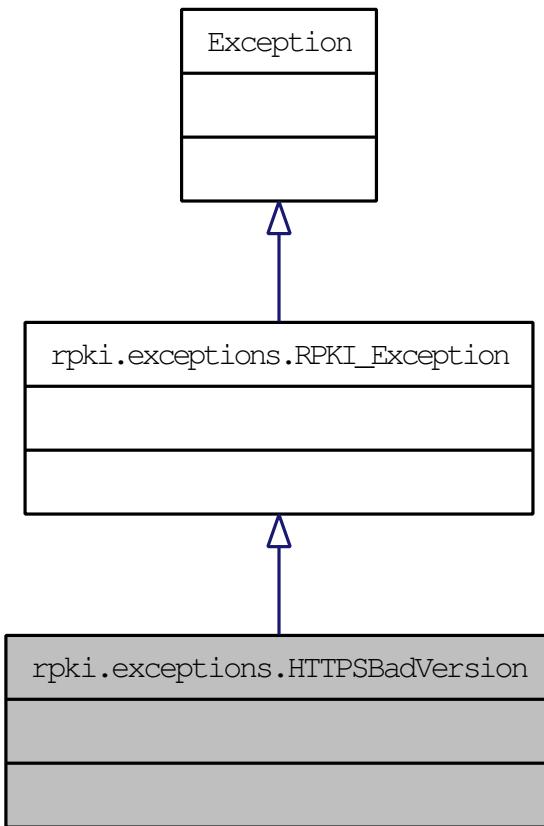
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.77 rpkி.exceptions.HTTPSBadVersion Class Reference

Inherits [rpkி::exceptions::RPKI_Exception](#).

Collaboration diagram for rpkி.exceptions.HTTPSBadVersion:



10.77.1 Detailed Description

HTTPS couldn't parse HTTP version.

Definition at line 287 of file exceptions.py.

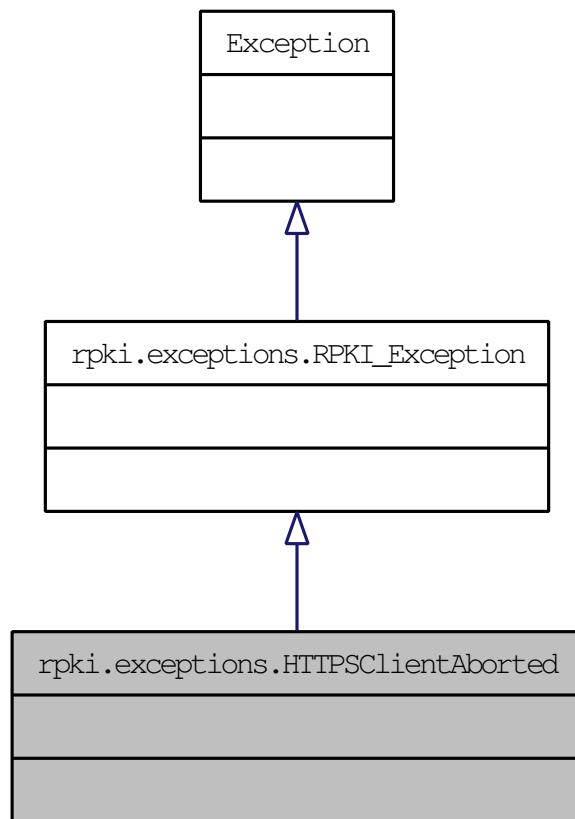
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.78 rpki.exceptions.HTTPSClientAborted Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.HTTPSClientAborted:



10.78.1 Detailed Description

HTTPS client connection closed while in request-sent state.

Definition at line 252 of file `exceptions.py`.

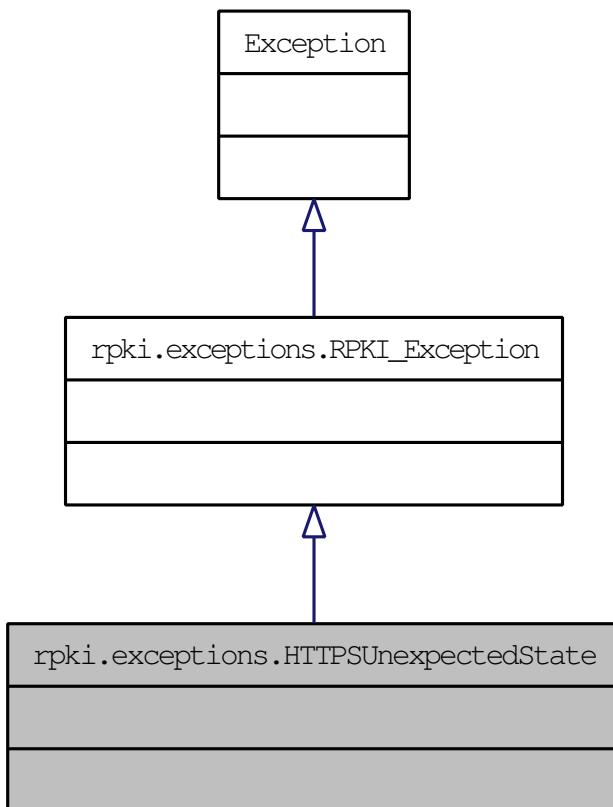
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.79 rpki.exceptions.HTTPSUnexpectedState Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.HTTPSUnexpectedState:



10.79.1 Detailed Description

HTTPS event occurred in an unexpected state.

Definition at line 282 of file `exceptions.py`.

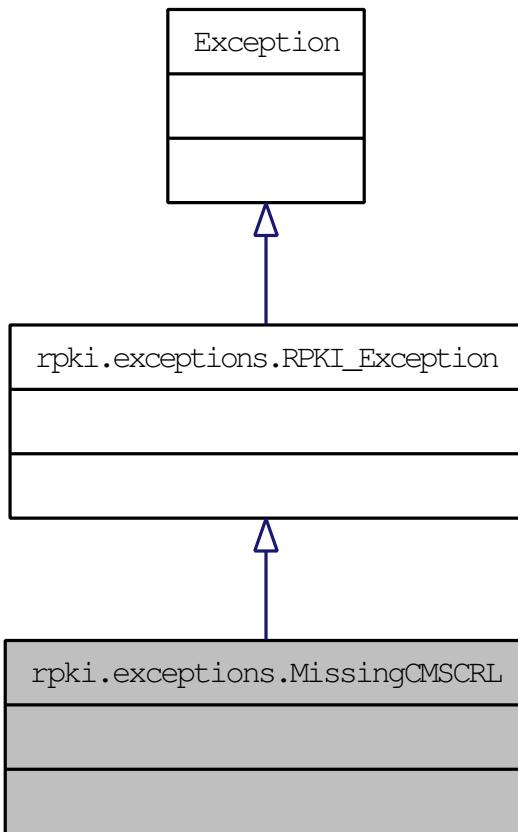
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.80 rpki.exceptions.MissingCMSCRL Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.MissingCMSCRL:



10.80.1 Detailed Description

Didn't receive CMS CRL when expecting one.

Definition at line 207 of file exceptions.py.

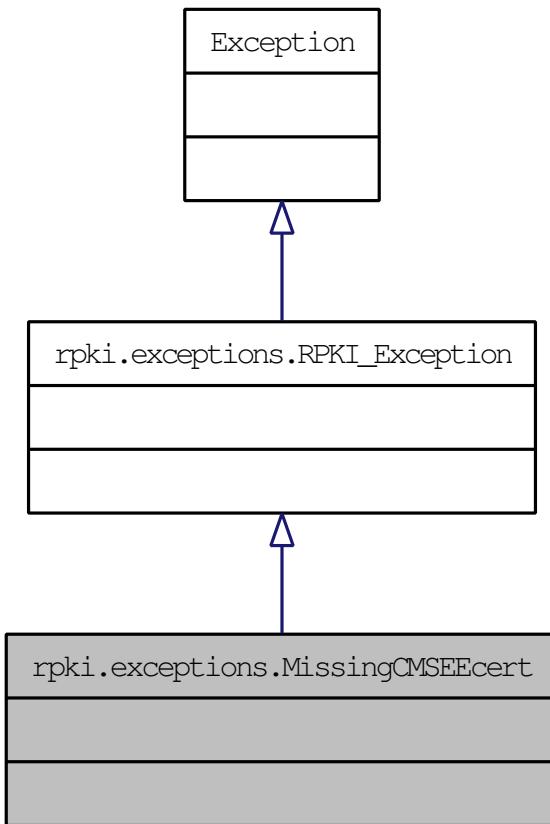
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.81 rpkி.exceptions.MissingCMSEEcrt Class Reference

Inherits [rpkி::exceptions::RPKI_Exception](#).

Collaboration diagram for rpkி.exceptions.MissingCMSEEcrt:



10.81.1 Detailed Description

Didn't receive CMS EE cert when expecting one.

Definition at line 202 of file exceptions.py.

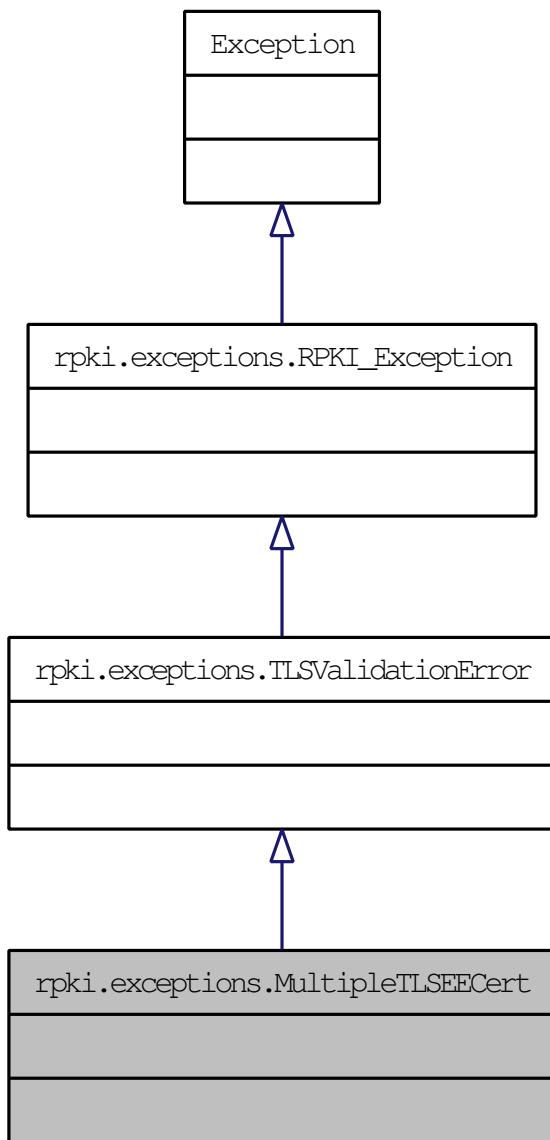
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.82 rpki.exceptions.MultipleTLSEECert Class Reference

Inherits [rpki::exceptions::TLSValidationError](#).

Collaboration diagram for rpki.exceptions.MultipleTLSEECert:



10.82.1 Detailed Description

Received more than one TLS EE certificate.

Definition at line 172 of file exceptions.py.

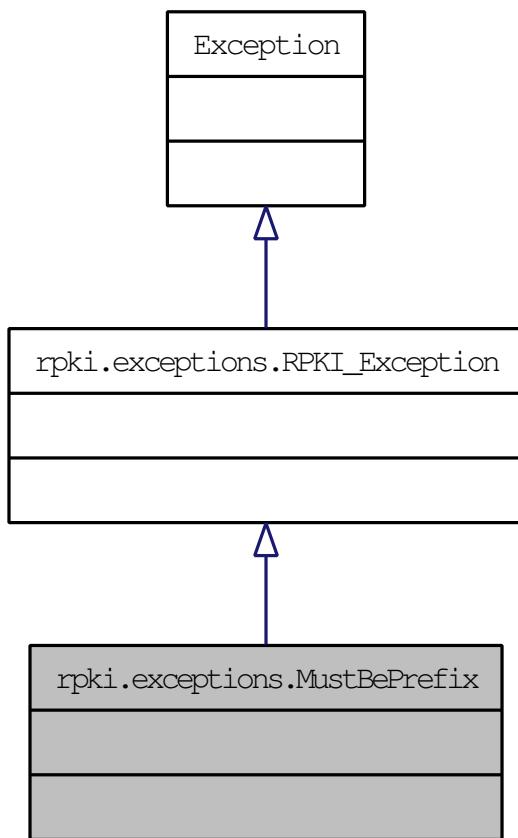
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.83 rpki.exceptions.MustBePrefix Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.MustBePrefix:



10.83.1 Detailed Description

Resource range cannot be expressed as a prefix.

Definition at line 162 of file exceptions.py.

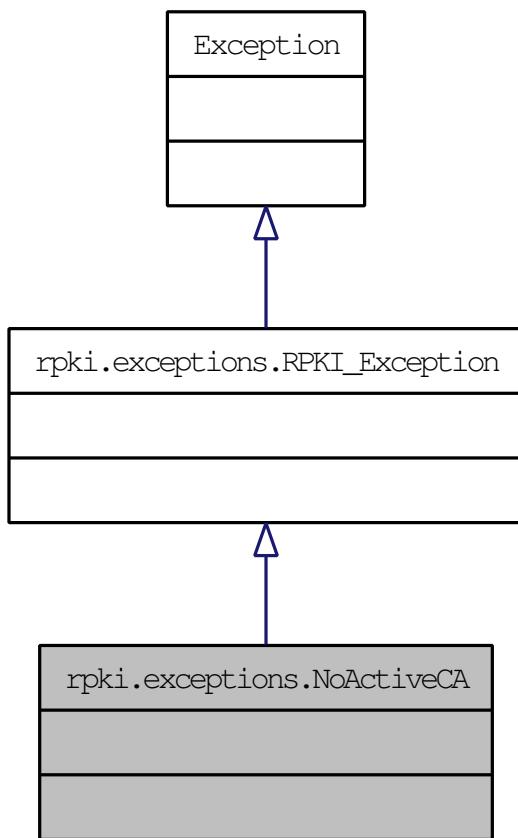
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.84 rpki.exceptions.NoActiveCA Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.NoActiveCA:



10.84.1 Detailed Description

No active ca_detail for specified class.

Definition at line 227 of file exceptions.py.

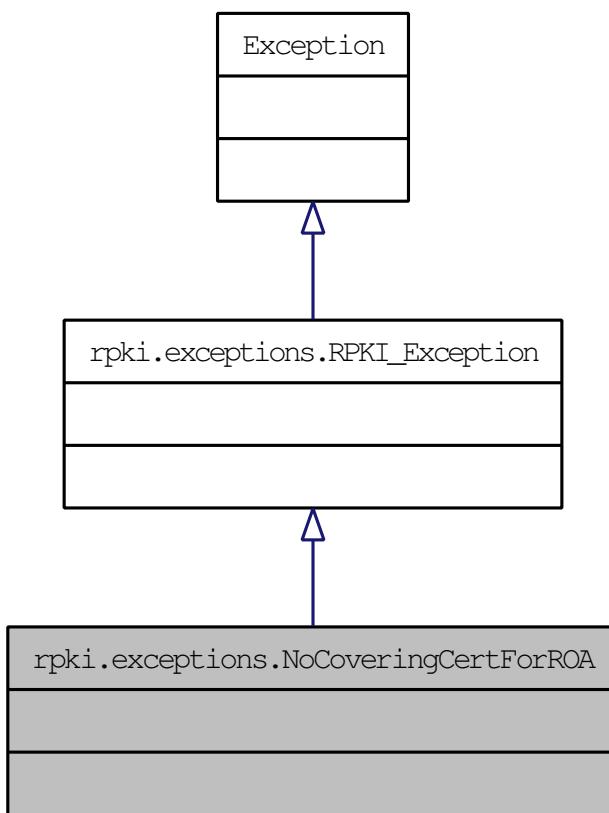
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.85 rpki.exceptions.NoCoveringCertForROA Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.NoCoveringCertForROA:



10.85.1 Detailed Description

Couldn't find a covering certificate to generate ROA.

Definition at line 272 of file exceptions.py.

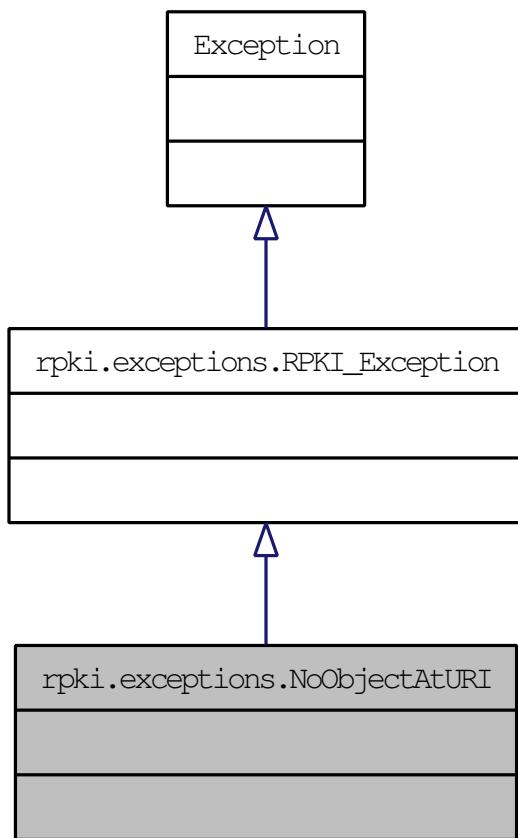
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.86 rpki.exceptions.NoObjectAtURI Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.NoObjectAtURI:



10.86.1 Detailed Description

No object published at specified URI.

Definition at line 297 of file exceptions.py.

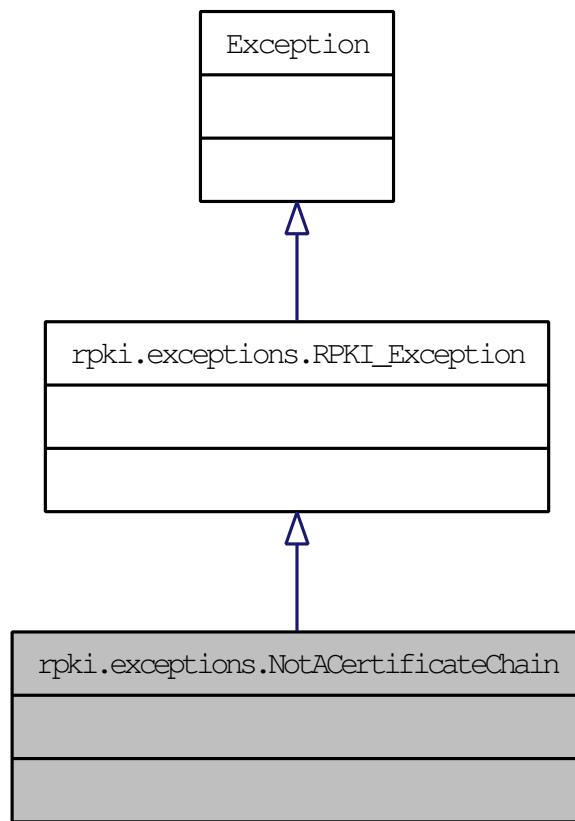
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.87 rpki.exceptions.NotACertificateChain Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.NotACertificateChain:



10.87.1 Detailed Description

Certificates don't form a proper chain.

Definition at line 82 of file exceptions.py.

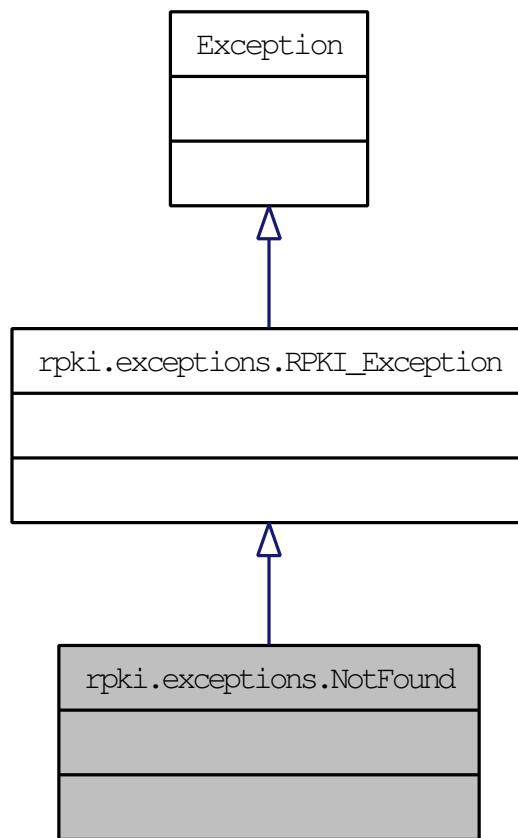
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.88 rpki.exceptions.NotFound Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.NotFound:



10.88.1 Detailed Description

Object not found in database.

Definition at line 157 of file exceptions.py.

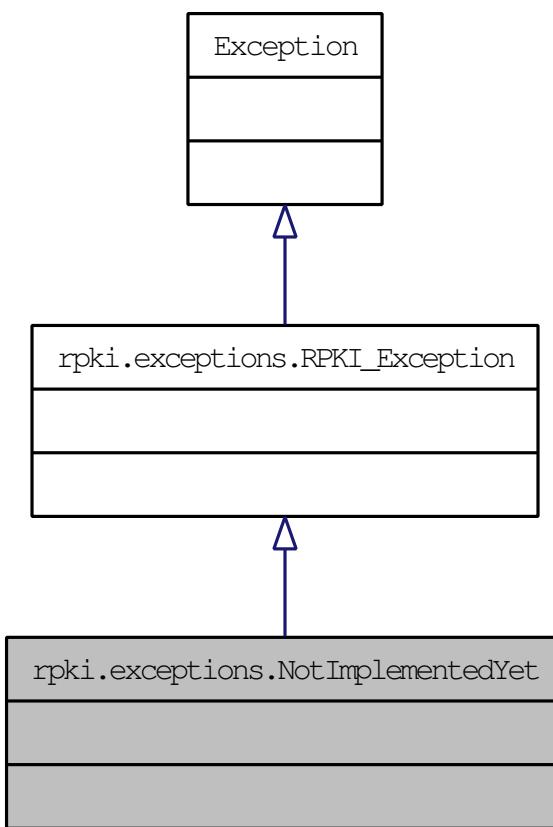
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.89 rpki.exceptions.NotImplementedYet Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.NotImplementedYet:



10.89.1 Detailed Description

Internal error -- not implemented yet.

Definition at line 102 of file exceptions.py.

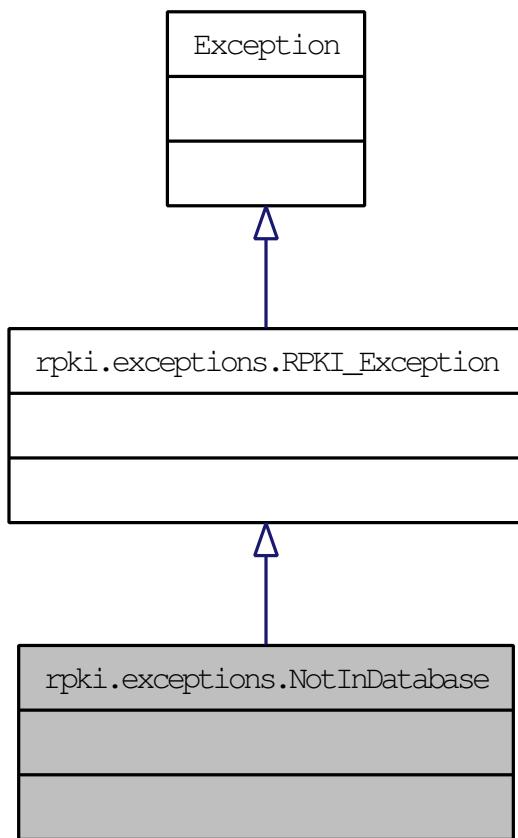
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.90 rpki.exceptions.NotInDatabase Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.NotInDatabase:



10.90.1 Detailed Description

Lookup failed for an object expected to be in the database.

Definition at line 40 of file exceptions.py.

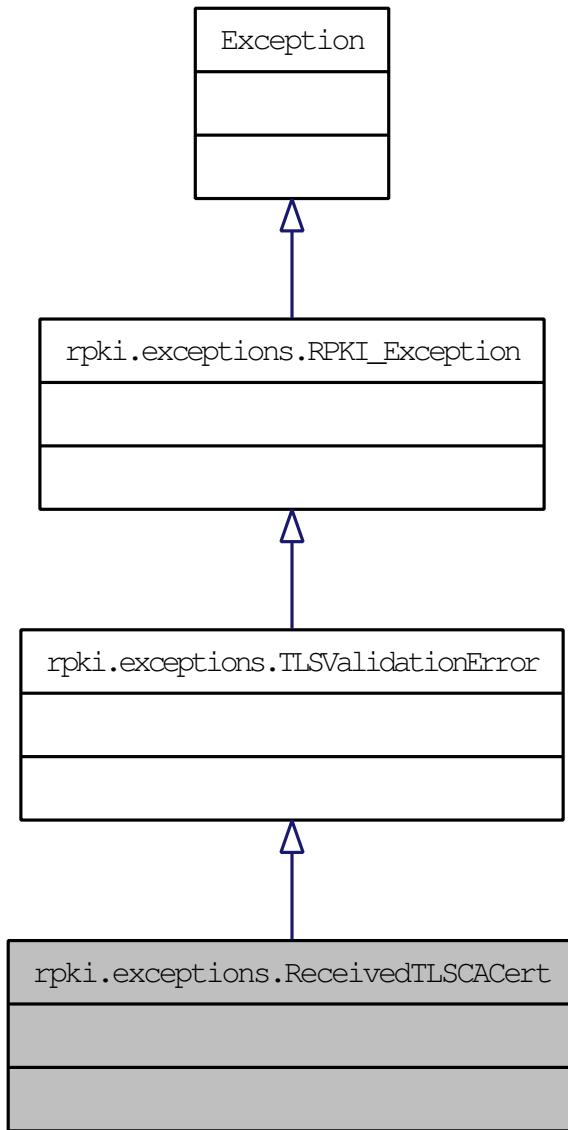
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.91 rpki.exceptions.ReceivedTLSCACert Class Reference

Inherits [rpki::exceptions::TLSValidationError](#).

Collaboration diagram for rpki.exceptions.ReceivedTLSCACert:



10.91.1 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:

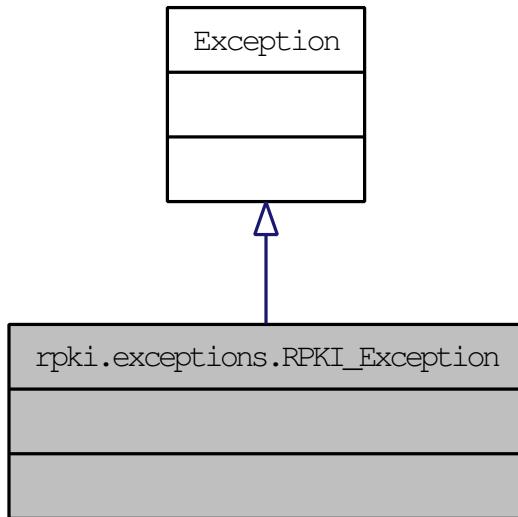
- [exceptions.py \(2907\)](#)

10.92 rpkி.exceptions.RPKI_Exception Class Reference

Inherits [Exception](#).

Inherited by [rpkி.exceptions.BadClassNameSyntax](#), [rpkி.exceptions.BadClientURL](#),
[rpkி.exceptions.BadContactURL](#), [rpkி.exceptions.BadExtension](#),
[rpkி.exceptions.BadIRDBReply](#), [rpkி.exceptions.BadIssueResponse](#),
[rpkி.exceptions.BadPKCS10](#), [rpkி.exceptions.BadPublicationReply](#),
[rpkி.exceptions.BadQuery](#), [rpkி.exceptions.BadSender](#),
[rpkième. exceptions.BadStatusCodes](#), [rpkième. exceptions.BadURISyntax](#),
[rpkième. exceptions.BSCNotFound](#), [rpkième. exceptions.BSCNotReady](#),
[rpkième. exceptions.ChildNotFound](#), [rpkième. exceptions.ClassNameMismatch](#),
[rpkième. exceptions.ClassNameUnknown](#), [rpkième. exceptions.ClientNotFound](#),
[rpkième. exceptions.CMSContentNotSet](#), [rpkième. exceptions.CMSCRLNotSet](#),
[rpkième. exceptions.CMSVerificationFailed](#), [rpkième. exceptions.DBConsistencyError](#),
[rpkième. exceptions.DERObjectConversionError](#), [rpkième. exceptions.DuplicateObject](#),
[rpkième. exceptions.EmptyPEM](#), [rpkième. exceptions.EmptyROAPrefixList](#),
[rpkième. exceptions.ForbiddenURI](#), [rpkième. exceptions.HandleTranslationError](#),
[rpkième. exceptions.HTTPRequestFailed](#), [rpkième. exceptions.HTTPSBadVersion](#),
[rpkième. exceptions.HTTPSClientAborted](#), [rpkième. exceptions.HTTPSUnexpectedState](#),
[rpkième. exceptions.MissingCMSCRL](#), [rpkième. exceptions.MissingCMSEEcert](#),
[rpkième. exceptions.MustBePrefix](#), [rpkième. exceptions.NoActiveCA](#),
[rpkième. exceptions.NoCoveringCertForROA](#), [rpkième. exceptions.NoObjectAtURI](#),
[rpkième. exceptions.NotACertificateChain](#), [rpkième. exceptions.NotFound](#),
[rpkième. exceptions.NotImplementedYet](#), [rpkième. exceptions.NotInDatabase](#),
[rpkième. exceptions.ServerShuttingDown](#), [rpkième. exceptions.SKIMismatch](#),
[rpkième. exceptions.SubprocessError](#), [rpkième. exceptions.TLSValidation](#),
[rpkième. exceptions.UnexpectedCMSCerts](#), [rpkième. exceptions.UnexpectedCMSCRLs](#),
[rpkième. exceptions.UnparsableCMSDER](#), [rpkième. exceptions.UpstreamError](#), and
[rpkième. exceptions.WrongEContentType](#).

Collaboration diagram for rpki.exceptions.RPKI_Exception:



10.92.1 Detailed Description

Base class for RPKI exceptions.

Definition at line 35 of file exceptions.py.

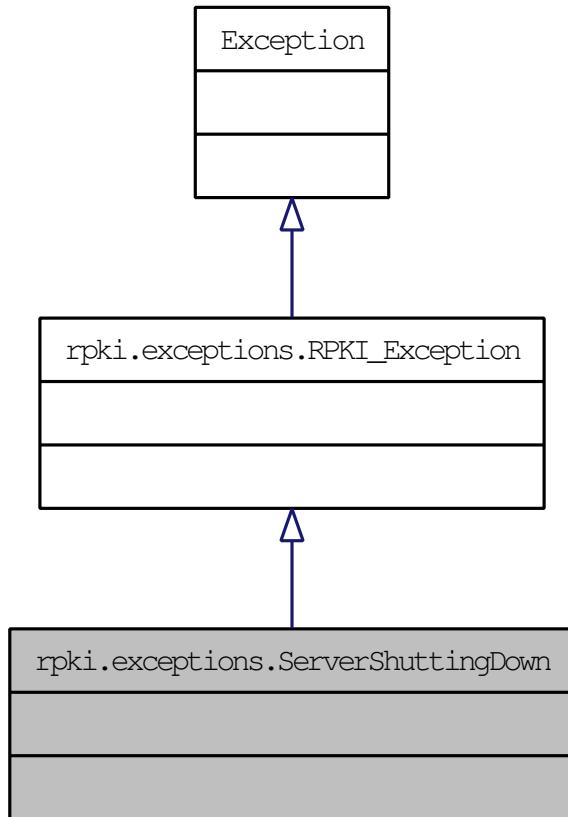
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.93 rpki.exceptions.ServerShuttingDown Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpkி.exceptions.ServerShuttingDown:



10.93.1 Detailed Description

Server is shutting down.

Definition at line 222 of file exceptions.py.

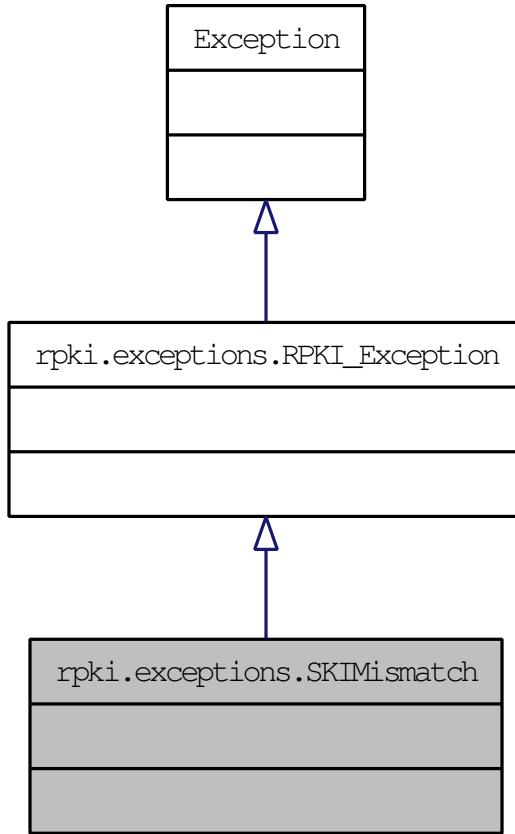
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.94 rpkி.exceptions.SKIMismatch Class Reference

Inherits [rpkி::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.SKIMismatch:



10.94.1 Detailed Description

SKI value in response does not match request.

Definition at line 142 of file exceptions.py.

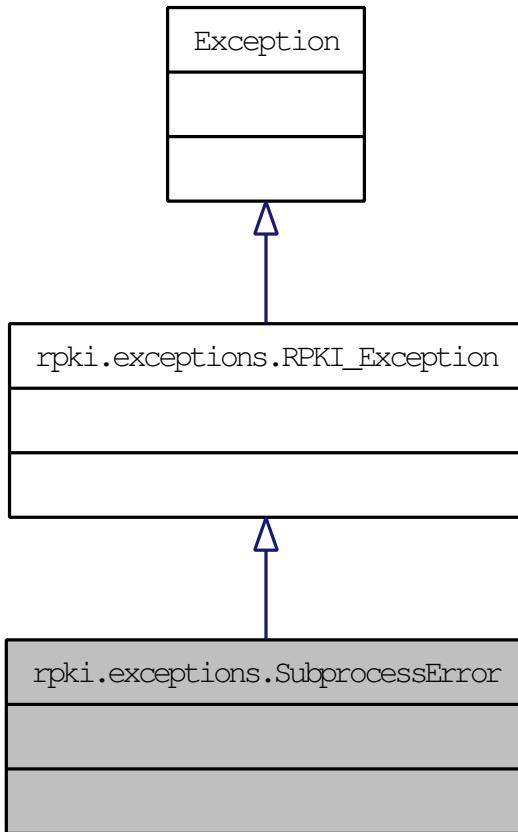
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.95 rpki.exceptions.SubprocessError Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.SubprocessError:



10.95.1 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:

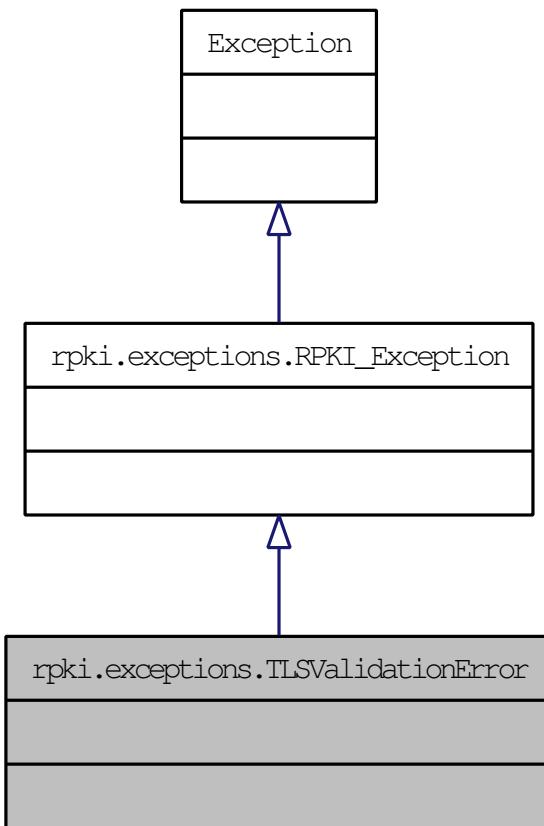
- [exceptions.py \(2907\)](#)

10.96 rpki.exceptions.TLSValidationError Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Inherited by [rpkி.exceptions.MultipleTLSEECert](#), and [rpkி.exceptions.ReceivedTLSCACert](#).

Collaboration diagram for rpkி.exceptions.TLSValidationException:



10.96.1 Detailed Description

TLS certificate validation error.

Definition at line 167 of file exceptions.py.

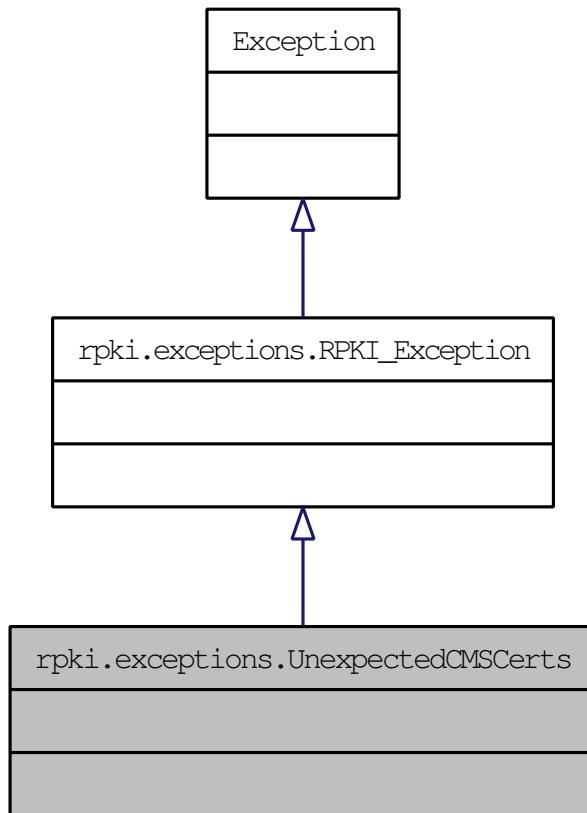
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.97 rpkி.exceptions.UnexpectedCMSCerts Class Reference

Inherits [rpkி::exceptions::RPKI_Exception](#).

Collaboration diagram for rpkி.exceptions.UnexpectedCMSCerts:



10.97.1 Detailed Description

Received CMS certs when not expecting any.

Definition at line 192 of file exceptions.py.

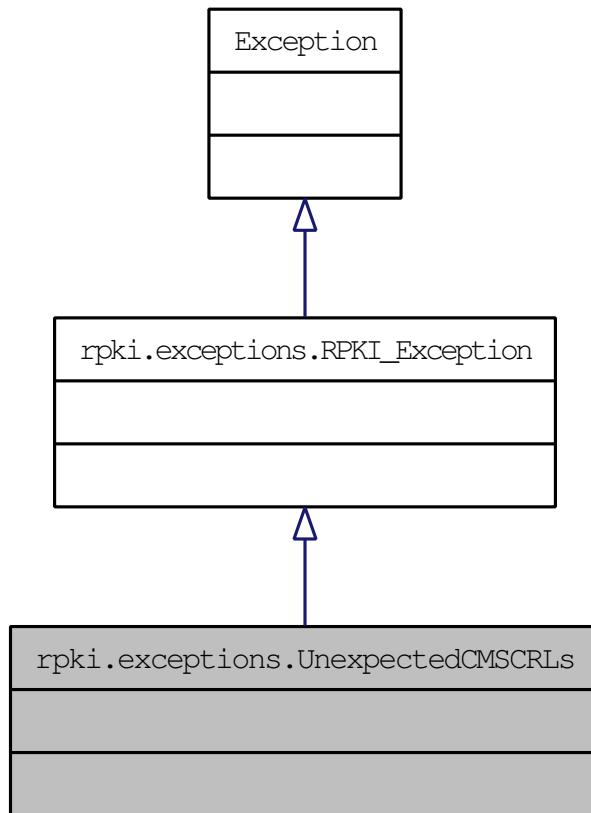
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.98 rpki.exceptions.UnexpectedCMSCRLs Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.UnexpectedCMSCRLs:



10.98.1 Detailed Description

Received CMS CRLs when not expecting any.

Definition at line 197 of file `exceptions.py`.

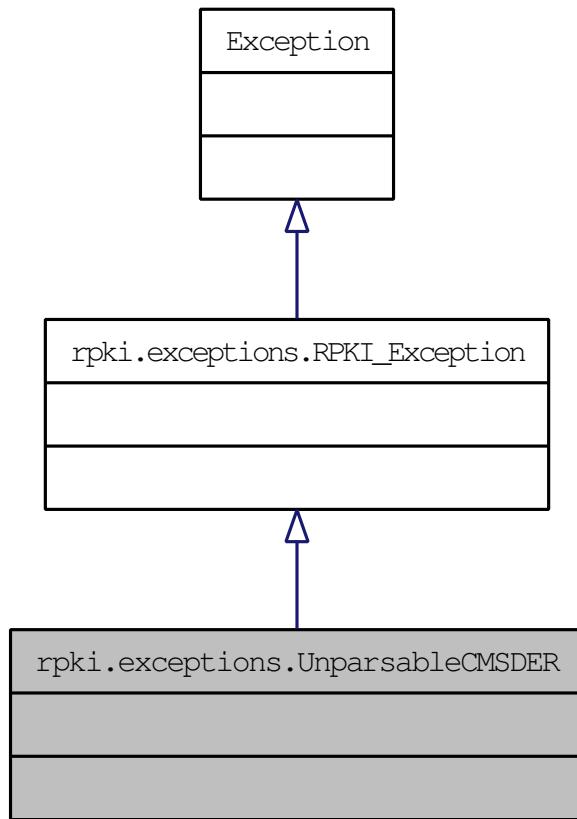
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.99 rpki.exceptions.UnparsableCMDSER Class Reference

Inherits [rpki::exceptions::RPKI_Exception](#).

Collaboration diagram for rpki.exceptions.UnparsableCMDSER:



10.99.1 Detailed Description

Alleged CMS DER wasn't parsable.

Definition at line 212 of file exceptions.py.

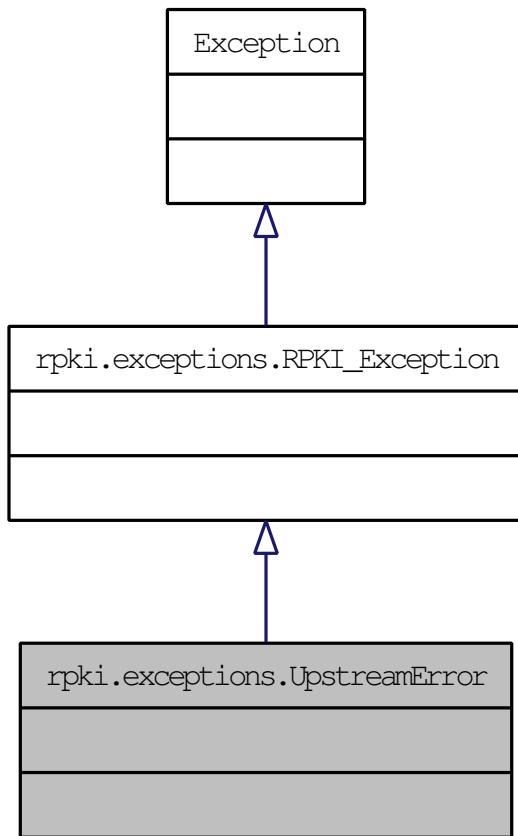
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.100 rpkி.exceptions.UpstreamError Class Reference

Inherits [rpkி::exceptions::RPKI_Exception](#).

Collaboration diagram for rpkி.exceptions.UpstreamError:



10.100.1 Detailed Description

Received an error from upstream.

Definition at line 112 of file exceptions.py.

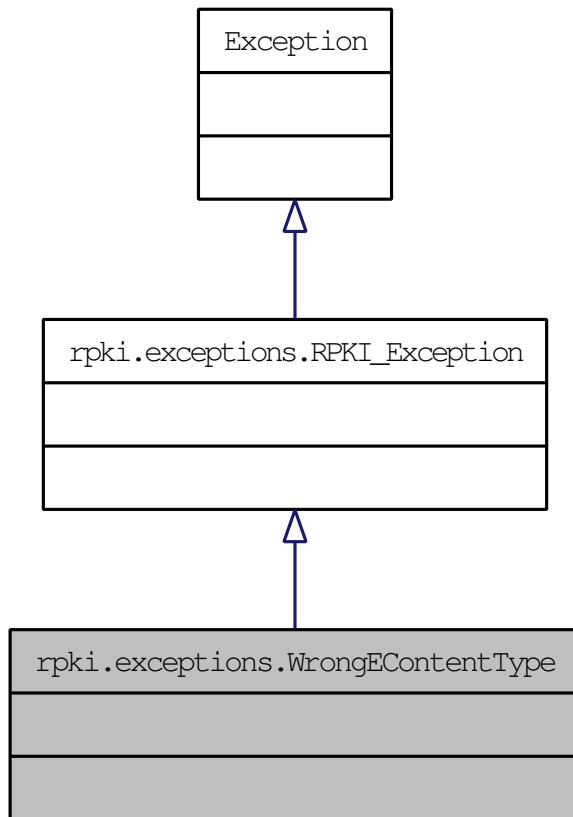
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.101 rpkி.exceptions.WrongEContentType Class Reference

Inherits [rpkி::exceptions::RPKI_Exception](#).

Collaboration diagram for rpkி.exceptions.WrongEContentType:



10.101.1 Detailed Description

Received wrong CMS eContentType.

Definition at line 182 of file exceptions.py.

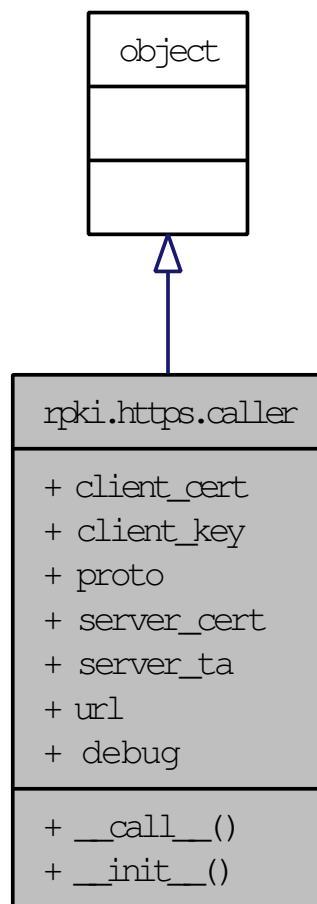
The documentation for this class was generated from the following file:

- [exceptions.py \(2907\)](#)

10.102 rpkি.https.caller Class Reference

Inherits [object](#).

Collaboration diagram for rpkি.https.caller:



Public Member Functions

- def `__call__`
- def `__init__`

Public Attributes

- `client_oert`

- [client_key](#)
- [proto](#)
- [server_cert](#)
- [server_ta](#)
- [url](#)

Static Public Attributes

- [debug](#) = False

10.102.1 Detailed Description

Handle client-side mechanics for protocols based on HTTPS, CMS, and rpkি. xml_utils. Calling sequence is intended to nest within rpkি. async.sync_wrapper.

Definition at line 1105 of file https.py.

10.102.2 Member Function Documentation

10.102.2.1 def rpkি.https.caller.__call__ (*self*, *cb*, *eb*, *pdu*s)

Definition at line 1124 of file https.py.

10.102.2.2 def rpkি.https.caller.__init__ (*self*, *proto*, *client_key*, *client_cert*, *server_ta*, *server_cert*, *url*, *debug* = `None`)

Definition at line 1114 of file https.py.

10.102.3 Member Data Documentation

10.102.3.1 rpkি.https.caller.client_cert

Definition at line 1117 of file https.py.

10.102.3.2 rpki.https.caller.client_key

Definition at line 1116 of file https.py.

10.102.3.3 rpki.https.caller.debug = False [static]

Definition at line 1112 of file https.py.

10.102.3.4 rpki.https.caller.proto

Definition at line 1115 of file https.py.

10.102.3.5 rpki.https.caller.server_cert

Definition at line 1119 of file https.py.

10.102.3.6 rpki.https.caller.server_ta

Definition at line 1118 of file https.py.

10.102.3.7 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 \(3191\)](#)

10.103 rpki.https.http_client Class Reference

Inherits [rpki::https::http_stream](#).

Collaboration diagram for rpkি.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.

10.103.1 Detailed Description

HTTP (S) client stream.

Definition at line 759 of file https.py.

10.103.2 Member Function Documentation

10.103.2.1 def rpkি.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.

10.103.2.2 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.

10.103.2.3 def rpki.https.http_client.handle_connect (*self*)

Asyncore says socket has connected, configure TLS junk.

Definition at line 797 of file https.py.

10.103.2.4 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.

10.103.2.5 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.

10.103.2.6 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.

10.103.2.7 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.

10.103.2.8 def rpki.https.http_client.send_request (*self*, *msg*)

Queue up request message and kickstart connection.

Definition at line 845 of file https.py.

10.103.2.9 def rpki.https.http_client.set_state (*self*, *state*)

Set HTTP client connection state.

Definition at line 829 of file https.py.

10.103.2.10 def rpki.https.http_client.start (*self*)

Create socket and request a connection.

Definition at line 785 of file https.py.

10.103.2.11 def rpki.https.http_client.tls_connect (*self*)

Initialize client side of TLS.

Definition at line 814 of file https.py.

10.103.3 Member Data Documentation**10.103.3.1 rpki.https.http_client.af**

Definition at line 783 of file https.py.

10.103.3.2 rpki.https.http_client.cert

Definition at line 780 of file https.py.

10.103.3.3 rpki.https.http_client.expect_close

Definition at line 779 of file https.py.

10.103.3.4 rpki.https.http_client.hostport

Definition at line 777 of file https.py.

10.103.3.5 rpki.https.http_client.key

Definition at line 781 of file https.py.

10.103.3.6 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.

10.103.3.7 rpki.https.http_client.queue

Definition at line 776 of file https.py.

10.103.3.8 rpki.https.http_client.retry_read

Reimplemented from [rpki.https.http_stream](#).

Definition at line 821 of file https.py.

10.103.3.9 rpki.https.http_client.retry_write

Reimplemented from [rpki.https.http_stream](#).

Definition at line 823 of file https.py.

10.103.3.10 rpki.https.http_client.state

Definition at line 778 of file https.py.

10.103.3.11 rpki.https.http_client.ta

Definition at line 782 of file https.py.

10.103.3.12 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.

10.103.3.13 rpki.https.http_client.tls

Reimplemented from [rpki.https.http_stream](#).

Definition at line 802 of file https.py.

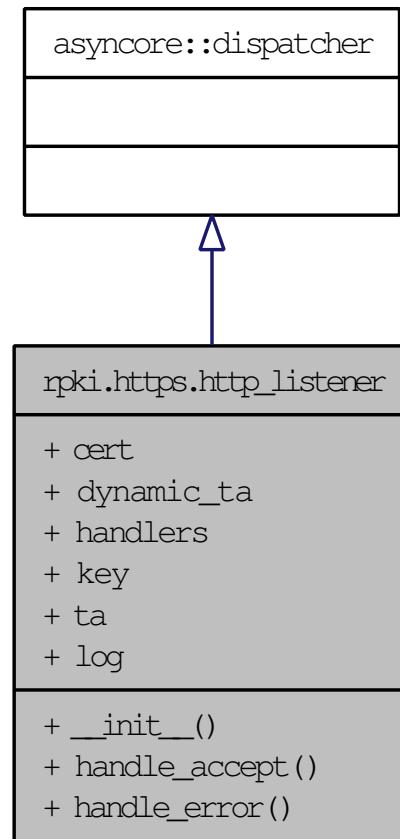
The documentation for this class was generated from the following file:

- [https.py \(3191\)](#)

10.104 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

10.104.1 Detailed Description

Listener for incoming HTTP(S) connections.

Definition at line 707 of file https.py.

10.104.2 Member Function Documentation

10.104.2.1 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.

10.104.2.2 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.

10.104.2.3 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.

10.104.3 Member Data Documentation**10.104.3.1 rpki.https.http_listener.cert**

Definition at line 718 of file https.py.

10.104.3.2 rpki.https.http_listener.dynamic_ta

Definition at line 721 of file https.py.

10.104.3.3 rpki.https.http_listener.handlers

Definition at line 717 of file https.py.

10.104.3.4 rpki.https.http_listener.key

Definition at line 719 of file https.py.

10.104.3.5 rpki.https.http_listener.log = log_method [static]

Definition at line 712 of file https.py.

10.104.3.6 rpki.https.http_listener.ta

Definition at line 720 of file https.py.

The documentation for this class was generated from the following file:

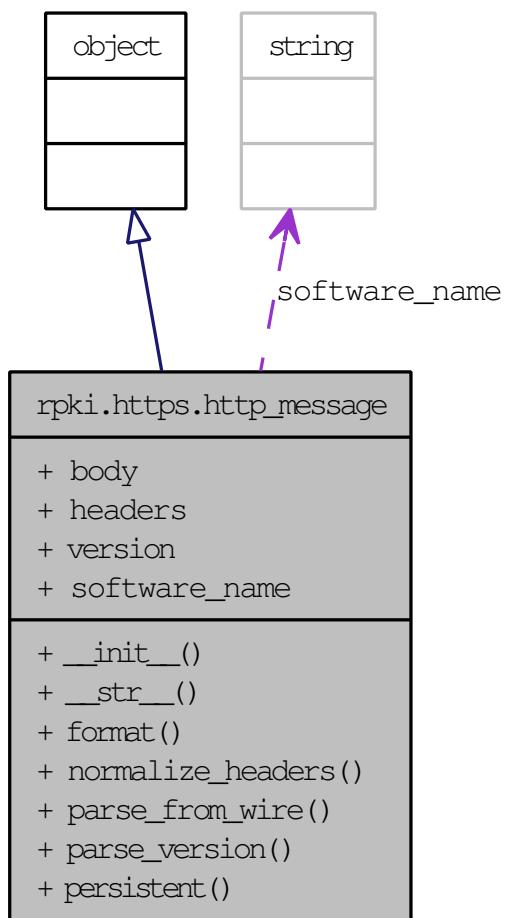
- [https.py \(3191\)](#)

10.105 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"

10.105.1 Detailed Description

Virtual class representing of one HTTP message.

Definition at line 90 of file https.py.

10.105.2 Member Function Documentation

10.105.2.1 def rpkি.https.http_message.`__init__`(*self*, *version* = `None`, *body* = `None`, *headers* = `None`)

Definition at line 97 of file https.py.

10.105.2.2 def rpkি.https.http_message.`__str__`(*self*)

Definition at line 155 of file https.py.

10.105.2.3 def rpkি.https.http_message.format (*self*)

Format an outgoing HTTP message.

Definition at line 140 of file https.py.

10.105.2.4 def rpkি.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.

10.105.2.5 def rpkি.https.http_message.parse_from_wire (*cls*, *headers*)

Parse and normalize an incoming HTTP message.

Definition at line 126 of file https.py.

10.105.2.6 def rpkি.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.

10.105.2.7 def rpkি.https.http_message.persistent (*self*)

Figure out whether this HTTP message encourages a persistent connection.

Definition at line 166 of file https.py.

10.105.3 Member Data Documentation**10.105.3.1 rpki.https.http_message.body**

Definition at line 99 of file https.py.

10.105.3.2 rpki.https.http_message.headers

Definition at line 100 of file https.py.

10.105.3.3 string rpki.https.http_message.software_name = "ISC RPKI library" [static]

Definition at line 95 of file https.py.

10.105.3.4 rpki.https.http_message.version

Definition at line 98 of file https.py.

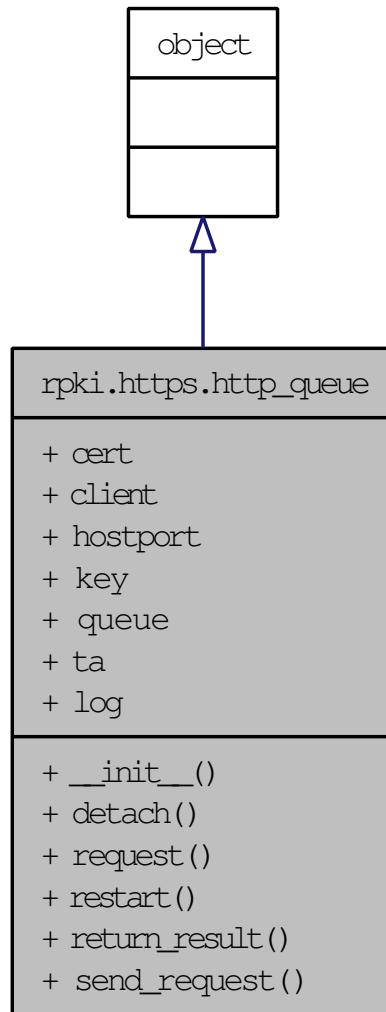
The documentation for this class was generated from the following file:

- [https.py \(3191\)](#)

10.106 rpki.https.http_queue Class Reference

Inherits [object](#).

Collaboration diagram for rpkি.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

10.106.1 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.

10.106.2 Member Function Documentation

10.106.2.1 def rpkি.https.http_queue.__init__ (self, hostport, cert = None, key = None, ta = ())

Definition at line 938 of file https.py.

10.106.2.2 def rpkি.https.http_queue.detach (self, client_)

Detatch a client from this queue. Silently ignores attempting to detatch 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.

10.106.2.3 def rpkি.https.http_queue.request (*self*, *requests*)

Append http_request object(s) to this queue.

Definition at line 948 of file https.py.

10.106.2.4 def rpkি.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.

10.106.2.5 def rpkি.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.

10.106.2.6 def rpkি.https.http_queue.send_request (*self*)

Kick out the next query in this queue, if any.

Definition at line 979 of file https.py.

10.106.3 Member Data Documentation**10.106.3.1 rpkি.https.http_queue.cert**

Definition at line 944 of file https.py.

10.106.3.2 rpki.https.http_queue.client

Definition at line 942 of file https.py.

10.106.3.3 rpki.https.http_queue.hostport

Definition at line 941 of file https.py.

10.106.3.4 rpki.https.http_queue.key

Definition at line 945 of file https.py.

10.106.3.5 rpki.https.http_queue.log = log_method [static]

Definition at line 936 of file https.py.

10.106.3.6 rpki.https.http_queue.queue

Definition at line 943 of file https.py.

10.106.3.7 rpki.https.http_queue.ta

Definition at line 946 of file https.py.

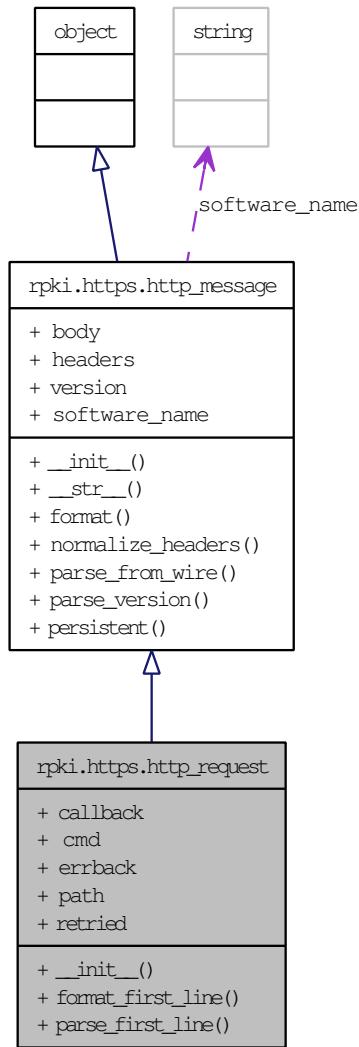
The documentation for this class was generated from the following file:

- [https.py \(3191\)](#)

10.107 rpki.https.http_request Class Reference

Inherits [rpki::https::http_message](#).

Collaboration diagram for rpkি.https.http_request:



Public Member Functions

- def [__init__](#)
- def [format_first_line](#)
- def [parse_first_line](#)

Public Attributes

- [callback](#)
- [cmd](#)
- [errback](#)
- [path](#)
- [retried](#)

10.107.1 Detailed Description

HTTP request message.

Definition at line 178 of file https.py.

10.107.2 Member Function Documentation

10.107.2.1 def rpkি.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.

10.107.2.2 def rpkি.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.

10.107.2.3 def rpkি.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.

10.107.3 Member Data Documentation**10.107.3.1 rpki.https.http_request.callback**

Definition at line 188 of file https.py.

10.107.3.2 rpki.https.http_request.cmd

Definition at line 186 of file https.py.

10.107.3.3 rpki.https.http_request.errback

Definition at line 189 of file https.py.

10.107.3.4 rpki.https.http_request.path

Definition at line 187 of file https.py.

10.107.3.5 rpki.https.http_request.retried

Definition at line 190 of file https.py.

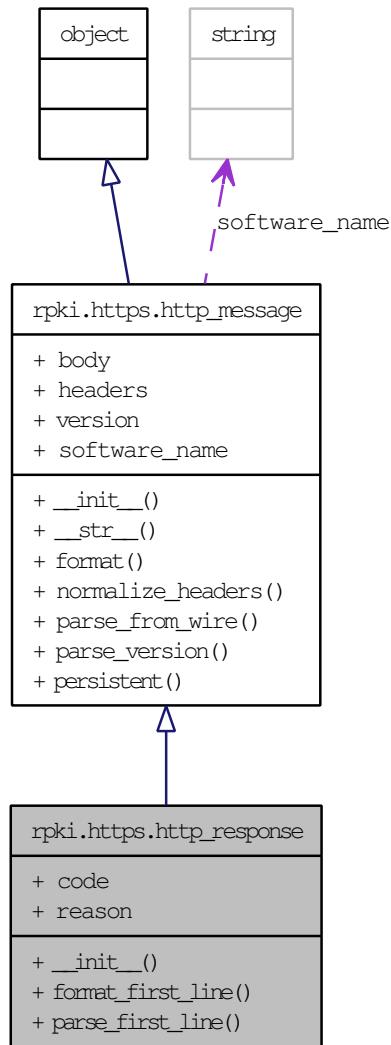
The documentation for this class was generated from the following file:

- [https.py \(3191\)](#)

10.108 rpki.https.http_response Class Reference

Inherits [rpki::https::http_message](#).

Collaboration diagram for rpkি.https.http_response:



Public Member Functions

- def `__init__`
- def `format_first_line`
- def `parse_first_line`

Public Attributes

- [code](#)
- [reason](#)

10.108.1 Detailed Description

HTTP response message.

Definition at line 208 of file https.py.

10.108.2 Member Function Documentation

10.108.2.1 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.

10.108.2.2 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.

10.108.2.3 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.

10.108.3 Member Data Documentation

10.108.3.1 rpki.https.http_response.code

Definition at line 215 of file https.py.

10.108.3.2 rpki.https.http_response.reason

Definition at line 216 of file https.py.

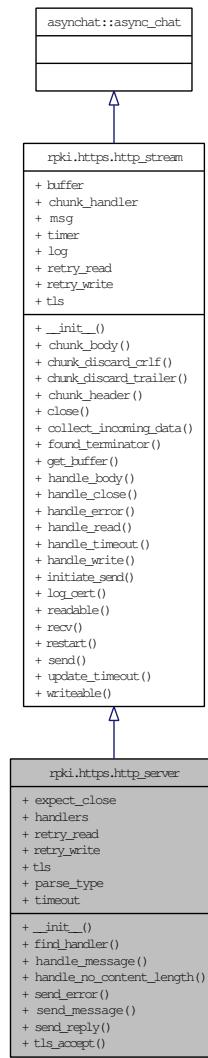
The documentation for this class was generated from the following file:

- [https.py \(3191\)](#)

10.109 rpki.https.http_server Class Reference

Inherits [rpki::https::http_stream](#).

Collaboration diagram for rpkি.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.

10.109.1 Detailed Description

HTTP (S) server stream.

Definition at line 561 of file https.py.

10.109.2 Member Function Documentation

10.109.2.1 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.

10.109.2.2 def rpki.https.http_server.find_handler (*self*, *path*)

Helper method to search *self.handlers*.

Definition at line 635 of file https.py.

10.109.2.3 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.

10.109.2.4 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.

10.109.2.5 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.

10.109.2.6 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.

10.109.2.7 def rpki.https.http_server.send_reply (*self, code, body*)

Send a reply to this request.

Definition at line 679 of file https.py.

10.109.2.8 def rpki.https.http_server.tls_accept (self)

Set up TLS for server side connection, handling all the whacky OpenSSL exceptions from TLS.

SSLErrorSSLException 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.

10.109.3 Member Data Documentation**10.109.3.1 rpki.https.http_server.expect_close**

Definition at line 578 of file https.py.

10.109.3.2 rpki.https.http_server.handlers

Definition at line 576 of file https.py.

10.109.3.3 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.

10.109.3.4 rpki.https.http_server.retry_read

Reimplemented from [rpki.https.http_stream](#).

Definition at line 613 of file https.py.

10.109.3.5 rpki.https.http_server.retry_write

Reimplemented from [rpki.https.http_stream](#).

Definition at line 615 of file https.py.

**10.109.3.6 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.

10.109.3.7 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:

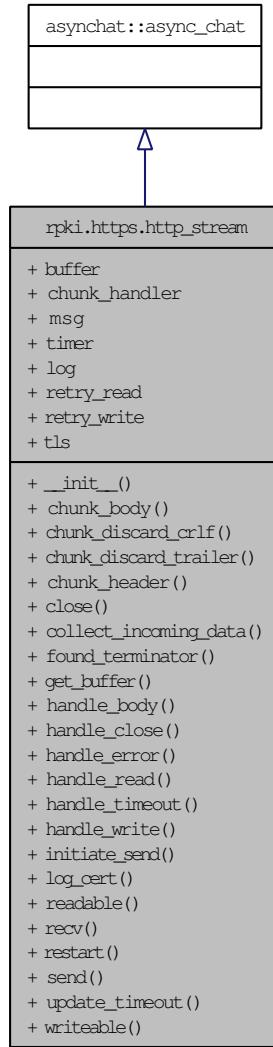
- [https.py \(3191\)](#)

10.110 rpki.https.http_stream Class Reference

Inherits [asynchat::async_chat](#).

Inherited by [rpki.https.http_client](#), and [rpki.https.http_server](#).

Collaboration diagram for rpkি.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

10.110.1 Detailed Description

Virtual class representing an HTTP message stream.

Definition at line 243 of file https.py.

10.110.2 Member Function Documentation**10.110.2.1 def rpkি.https.http_stream.__init__(self, sock = None)**

Definition at line 253 of file https.py.

10.110.2.2 def rpkি.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.

10.110.2.3 def rpkি.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.

10.110.2.4 def rpkি.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.

10.110.2.5 def rpkি.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.

10.110.2.6 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.

10.110.2.7 def rpki.https.http_stream.collect_incoming_data (*self*, *data*)

Buffer incoming data from asynchat.

Definition at line 279 of file https.py.

10.110.2.8 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.

10.110.2.9 def rpki.https.http_stream.get_buffer (*self*)

Consume data buffered from asynchat.

Definition at line 286 of file https.py.

10.110.2.10 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.

10.110.2.11 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.

10.110.2.12 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.

10.110.2.13 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.

10.110.2.14 def rpki.https.http_stream.handle_timeout (*self*)

Inactivity timer expired, close connection with prejudice.

Reimplemented in [rpkি.https.http_client](#).

Definition at line 399 of file https.py.

10.110.2.15 def rpkি.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.

10.110.2.16 def rpkি.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.

10.110.2.17 def rpkি.https.http_stream.log_cert (*self, tag, x*)

Log HTTPS certificates, if certificate debugging is enabled.

Definition at line 554 of file https.py.

10.110.2.18 def rpkি.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.

10.110.2.19 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.

10.110.2.20 def rpki.https.http_stream.restart (*self*)

(Re)start HTTP message parser, reset timer.

Definition at line 259 of file https.py.

10.110.2.21 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.

10.110.2.22 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.

10.110.2.23 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.

10.110.3 Member Data Documentation**10.110.3.1 rpki.https.http_stream.buffer**

Definition at line 255 of file https.py.

10.110.3.2 rpki.https.http_stream.chunk_handler

Definition at line 264 of file https.py.

10.110.3.3 rpki.https.http_stream.log = log_method [static]

Definition at line 248 of file https.py.

10.110.3.4 rpki.https.http_stream.msg

Definition at line 317 of file https.py.

10.110.3.5 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.

10.110.3.6 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.

10.110.3.7 rpki.https.http_stream.timer

Definition at line 256 of file https.py.

10.110.3.8 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.

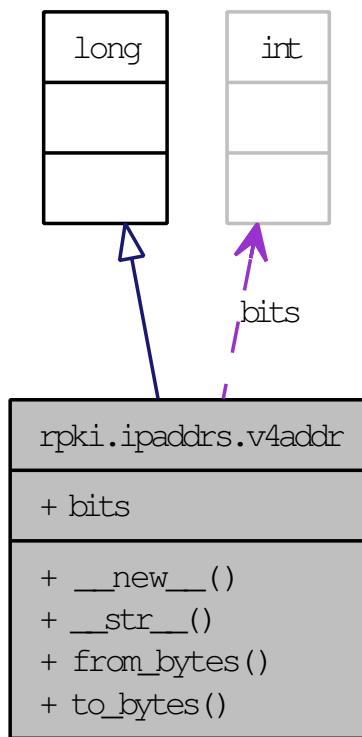
The documentation for this class was generated from the following file:

- [https.py \(3191\)](#)

10.111 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

10.111.1 Detailed Description

IPv4 address.

Derived from long, but supports IPv4 print syntax.

Definition at line 47 of file ipaddrs.py.

10.111.2 Member Function Documentation

10.111.2.1 def rpk.iipaddrs.v4addr.[__new__](#) (*cls, x*)

Construct a v4addr object.

Definition at line 56 of file ipaddrs.py.

10.111.2.2 def rpk.iipaddrs.v4addr.[__str__](#) (*self*)

Convert a v4addr object to string format.

Definition at line 74 of file ipaddrs.py.

10.111.2.3 def rpk.iipaddrs.v4addr.[from_bytes](#) (*cls, x*)

Convert from a raw byte string to a v4addr object.

Definition at line 70 of file ipaddrs.py.

10.111.2.4 def rpki.ipaddrs.v4addr.to_bytes (*self*)

Convert a v4addr object to a raw byte string.

Definition at line 65 of file ipaddrs.py.

10.111.3 Member Data Documentation**10.111.3.1 int rpki.ipaddrs.v4addr.bits = 32 [static]**

Definition at line 54 of file ipaddrs.py.

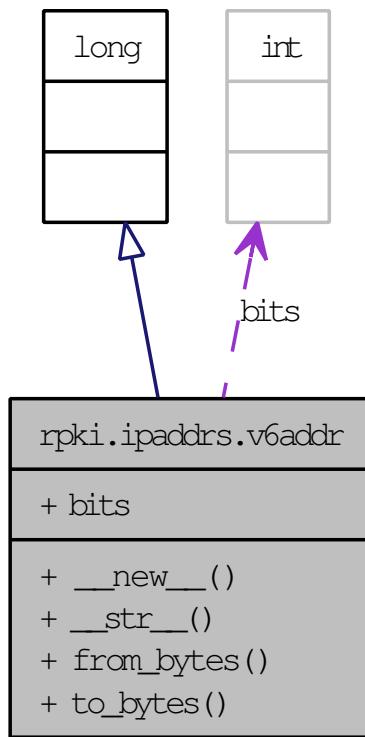
The documentation for this class was generated from the following file:

- [ipaddrs.py \(2424\)](#)

10.112 rpki.ipaddrs.v6addr Class Reference

Inherits [long](#).

Collaboration diagram for rpk.iipaddrs.v6addr:



Public Member Functions

- def `__new__`
- def `__str__`
- def `from_bytes`
- def `to_bytes`

Static Public Attributes

- int `bits` = 128

10.112.1 Detailed Description

IPv6 address.

Derived from `long`, but supports IPv6 print syntax.

Definition at line 78 of file ipaddrs.py.

10.112.2 Member Function Documentation

10.112.2.1 def rpk.iipaddrs.v6addr.__new__ (*cls*, *x*)

Construct a v6addr object.

Definition at line 87 of file ipaddrs.py.

10.112.2.2 def rpk.iipaddrs.v6addr.__str__ (*self*)

Convert a v6addr object to string format.

Definition at line 104 of file ipaddrs.py.

10.112.2.3 def rpk.iipaddrs.v6addr.from_bytes (*cls*, *x*)

Convert from a raw byte string to a v6addr object.

Definition at line 99 of file ipaddrs.py.

10.112.2.4 def rpk.iipaddrs.v6addr.to_bytes (*self*)

Convert a v6addr object to a raw byte string.

Definition at line 94 of file ipaddrs.py.

10.112.3 Member Data Documentation

10.112.3.1 int rpk.iipaddrs.v6addr.bits = 128 [static]

Definition at line 85 of file ipaddrs.py.

The documentation for this class was generated from the following file:

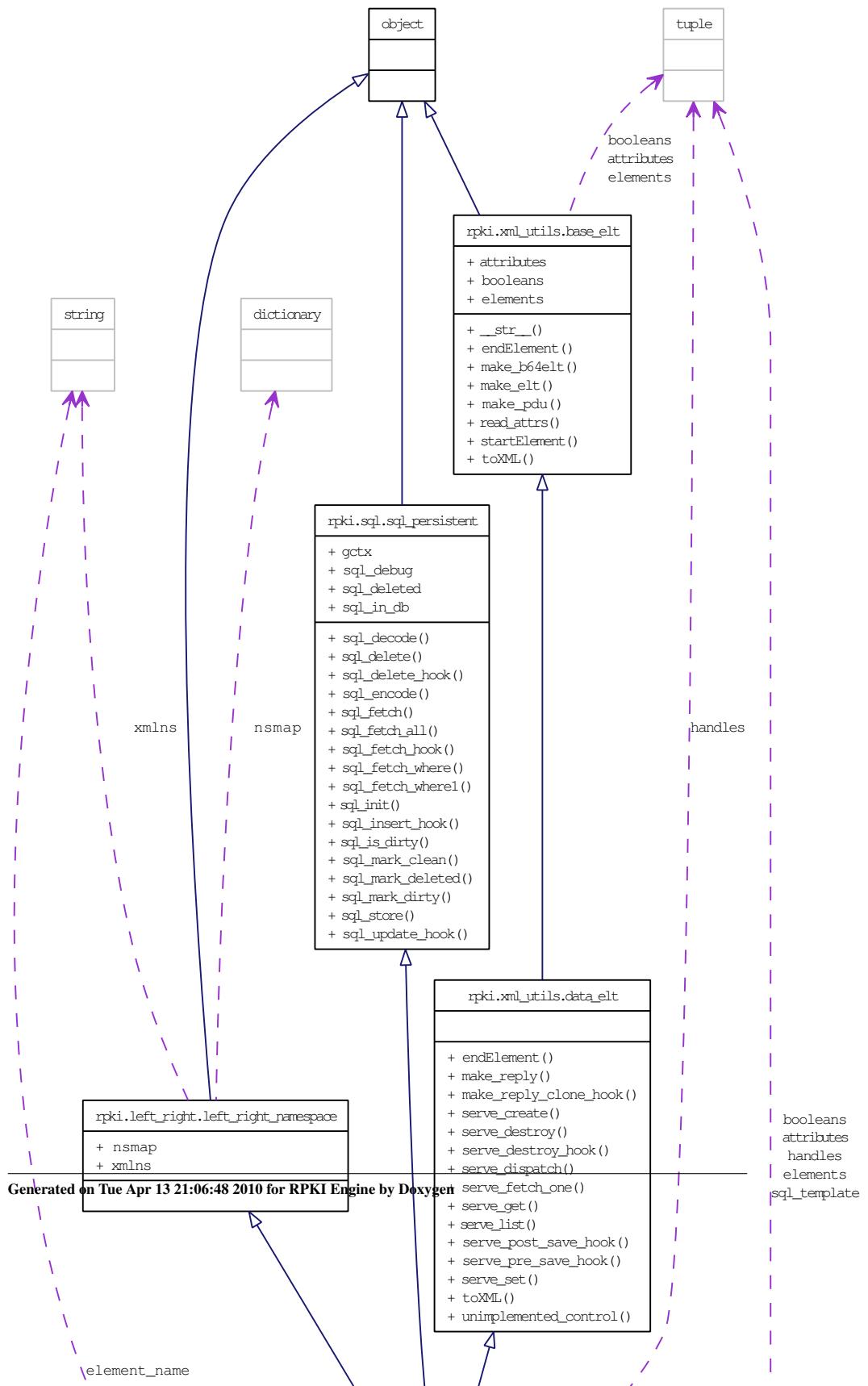
- [ipaddrs.py \(2424\)](#)

10.113 rpki.left_right.bsc_elt Class Reference

Inherits [rpki::left_right::data_elt](#).

Inherited by [irbe_cli.bsc_elt](#).

Collaboration diagram for rpk.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](#)

10.113.1 Detailed Description

`<bsc/>` (Business Signing Context) element.

Definition at line 526 of file left_right.py.

10.113.2 Member Function Documentation

10.113.2.1 def rpk.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.

10.113.2.2 def rpk.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.

10.113.2.3 def rpk.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.

10.113.2.4 def rpk.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 [rpk.left_right.data_elt](#).

Definition at line 561 of file left_right.py.

10.113.3 Member Data Documentation**10.113.3.1 tuple rpk.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 [rpk.xml_utils.base_elt](#).

Definition at line 532 of file left_right.py.

10.113.3.2 tuple rpk.left_right.bsc_elt.booleans = ("generate_keypair",) [static]

Boolean attributes (value "yes" or "no") for this element.

Reimplemented from [rpkি.xml_utils.base_elt](#).

Definition at line 534 of file left_right.py.

10.113.3.3 string rpkি.left_right.bsc_elt.element_name = "bsc" [static]

Definition at line 531 of file left_right.py.

10.113.3.4 tuple rpkি.left_right.bsc_elt.elements = ("signing_cert", "signing_cert_crl", "pkcs10_request") [static]

XML elements contained by this element.

Reimplemented from [rpkি.xml_utils.base_elt](#).

Definition at line 533 of file left_right.py.

10.113.3.5 tuple rpkি.left_right.bsc_elt.handles = (('self', self_elt),) [static]

Reimplemented from [rpkি.left_right.data_elt](#).

Definition at line 542 of file left_right.py.

10.113.3.6 rpkি.left_right.bsc_elt.pkcs10_request = None [static]

Definition at line 545 of file left_right.py.

10.113.3.7 rpkি.left_right.bsc_elt.private_key_id = None [static]

Definition at line 544 of file left_right.py.

10.113.3.8 rpkি.left_right.bsc_elt.signing_cert = None [static]

Reimplemented in [irbe_cli.bsc_elt](#).

Definition at line 546 of file left_right.py.

10.113.3.9 rpkি.left_right.bsc_elt.signing_cert_crl = None [static]

Reimplemented in [irbe_cli.bsc_elt](#).

Definition at line 547 of file left_right.py.

10.113.3.10 tuple rpkি.left_right.bsc_elt.sql_template [static]

Initial value:

```
rpkি.sql.template("bsc", "bsc_id", "bsc_handle",
                   "self_id", "hash_alg",
                   ("private_key_id", rpkি.x509.RSA),
                   ("pkcs10_request", rpkি.x509.PKCS10),
                   ("signing_cert", rpkি.x509.X509),
                   ("signing_cert_crl", rpkি.x509.CRL))
```

Definition at line 536 of file left_right.py.

The documentation for this class was generated from the following file:

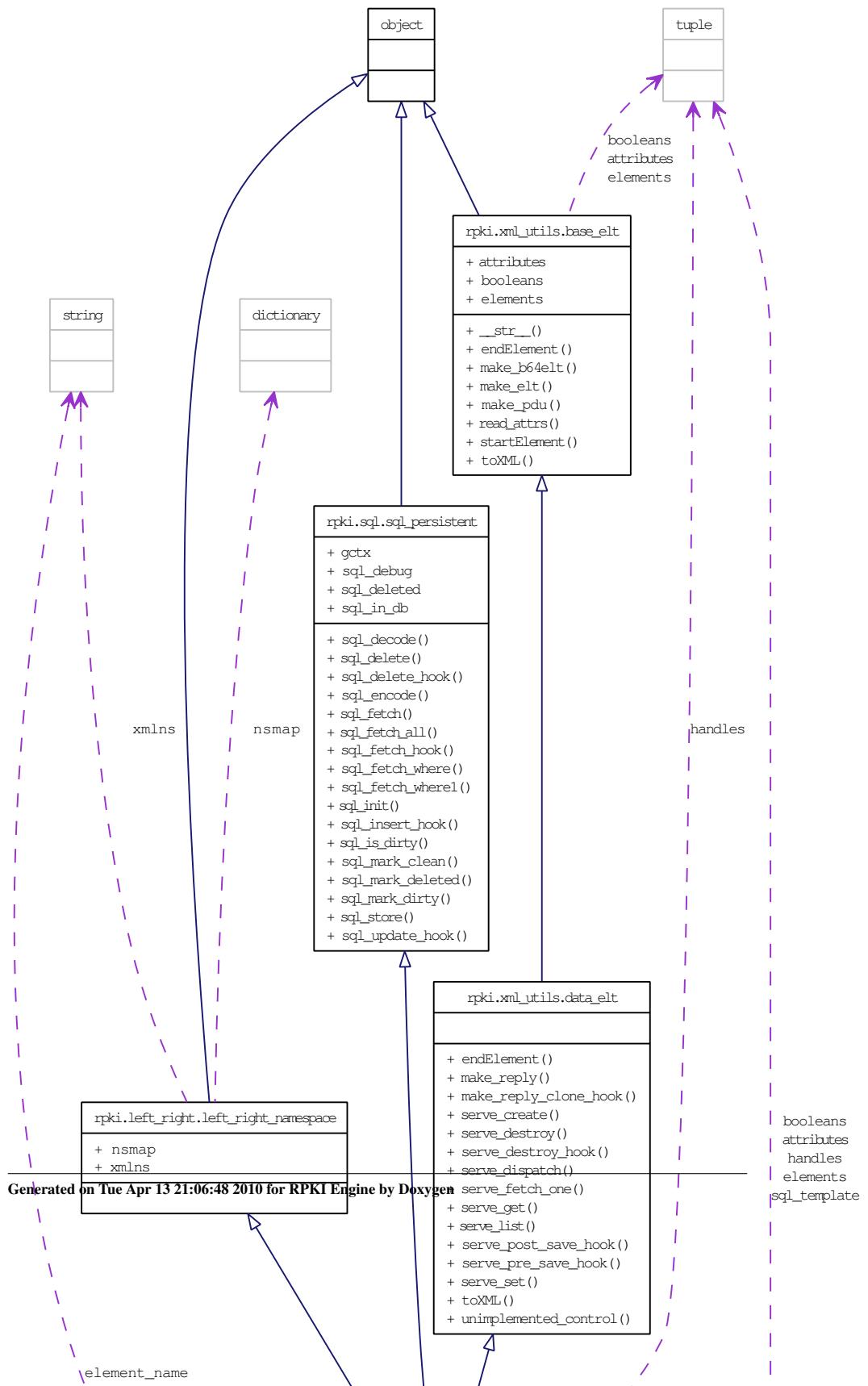
- [left_right.py \(3191\)](#)

10.114 rpkি.left_right.child_elt Class Reference

Inherits [rpkি::left_right::data_elt](#).

Inherited by [irbe_cli.child_elt](#).

Collaboration diagram for rpk.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.
- `bpk.cert` = None
- `bpk.glue` = None
- `clear_https_ta_cache` = False
- string `element_name` = "child"
- tuple `elements` = ("bpk.cert", "bpk.glue")
XML elements contained by this element.
- tuple `handles` = ((`"self"`, `self_elt`), (`"bsc"`, `bsc_elt`))
- tuple `sql_template`

10.114.1 Detailed Description

`<child/>` element.

Definition at line 805 of file left_right.py.

10.114.2 Member Function Documentation

10.114.2.1 def rpk.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.

10.114.2.2 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.

10.114.2.3 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.

10.114.2.4 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.

10.114.2.5 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.

10.114.2.6 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.

10.114.2.7 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.

10.114.3 Member Data Documentation**10.114.3.1 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.

10.114.3.2 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.

10.114.3.3 rpki.left_right.child_elt.bpkki_cert = None [static]

Definition at line 822 of file left_right.py.

10.114.3.4 rpki.left_right.child_elt.bpkki_glue = None [static]

Definition at line 823 of file left_right.py.

10.114.3.5 rpki.left_right.child_elt.clear_https_ta_cache = False [static]

Definition at line 824 of file left_right.py.

10.114.3.6 string rpki.left_right.child_elt.element_name = "child" [static]

Definition at line 810 of file left_right.py.

10.114.3.7 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.

10.114.3.8 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.

10.114.3.9 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:

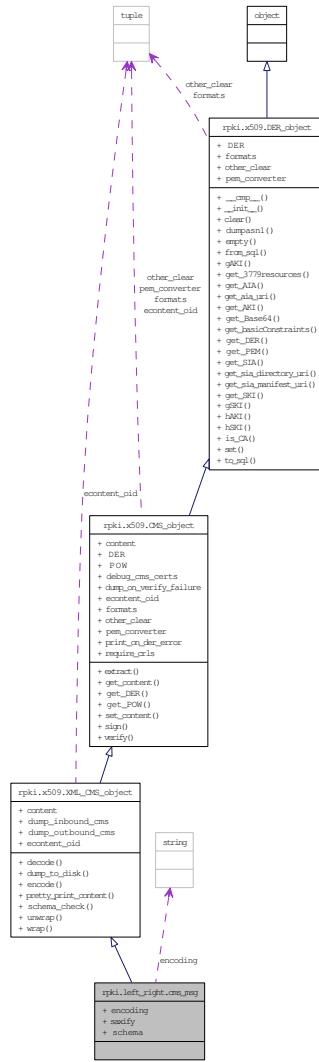
- [left_right.py \(3191\)](#)

10.115 rpki.left_right.cms_msg Class Reference

Inherits [rpki::x509::XML_CMS_object](#).

Inherited by [irbe_cli.left_right_cms_msg](#).

Collaboration diagram for rpk.left_right.cms_msg:



Static Public Attributes

- string **encoding** = "us-ascii"
- **saxify** = sax_handler.saxify
- **schema** = rpk.relaxng.left_right

10.115.1 Detailed Description

Class to hold a CMS-signed left-right PDU.

Definition at line 1120 of file `left_right.py`.

10.115.2 Member Data Documentation

10.115.2.1 string rpki.left_right.cms_msg.encoding = "us-ascii" [static]

Definition at line 1125 of file `left_right.py`.

10.115.2.2 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`.

10.115.2.3 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:

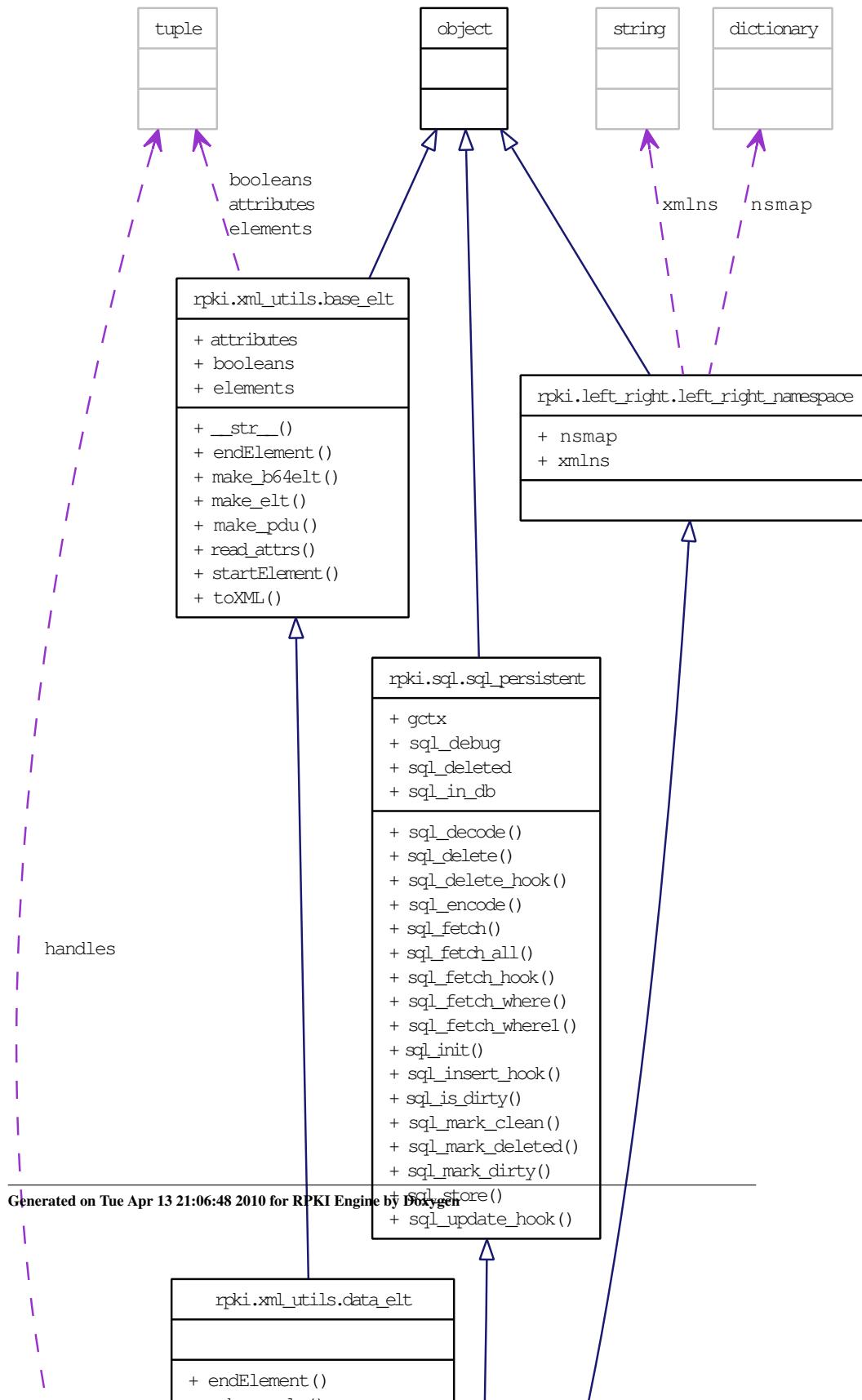
- [left_right.py \(3191\)](#)

10.116 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 rpk.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

10.116.1 Detailed Description

Virtual class for top-level left-right protocol data elements.

Definition at line 50 of file left_right.py.

10.116.2 Member Function Documentation

10.116.2.1 def rpk.left_right.data_elt.bsc (*self*)

Return BSC object to which this object links.

Definition at line 64 of file left_right.py.

10.116.2.2 def rpk.left_right.data_elt.make_reply_clone_hook (*self, r_pdu*)

Set handles when cloning, including `_id -> _handle` translation.

Reimplemented from [rpk.xml_utils.data_elt](#).

Definition at line 68 of file left_right.py.

10.116.2.3 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.

10.116.2.4 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.

10.116.2.5 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.

10.116.2.6 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.

10.116.2.7 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.

10.116.3 Member Data Documentation

10.116.3.1 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.

10.116.3.2 rpki.left_right.data_elt.self_handle = None [static]

Definition at line 58 of file left_right.py.

10.116.3.3 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:

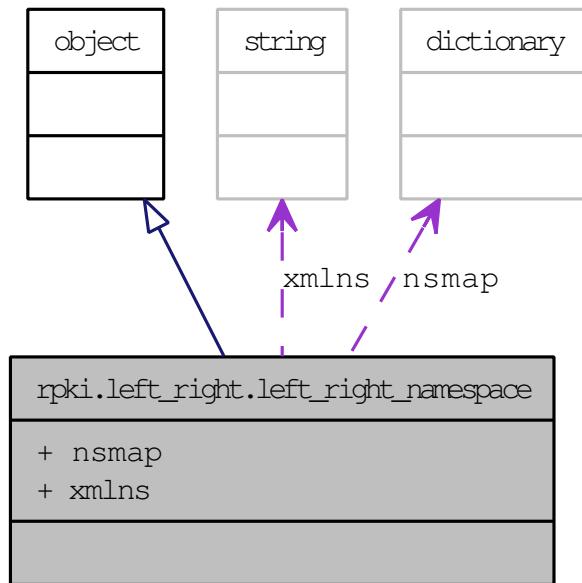
- [left_right.py \(3191\)](#)

10.117 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 rpk.left_right.left_right_namespace:



Static Public Attributes

- dictionary `nsmap` = { None : `xmlns` }
- string `xmlns` = "http://www.hactrn.net/uris/rpki/left-right-spec/"

10.117.1 Detailed Description

XML namespace parameters for left-right protocol.

Definition at line 42 of file `left_right.py`.

10.117.2 Member Data Documentation

10.117.2.1 dictionary `rpk.left_right.left_right_namespace.nsmap` = { None : `xmlns` } [static]

Definition at line 48 of file `left_right.py`.

```
10.117.2.2 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:

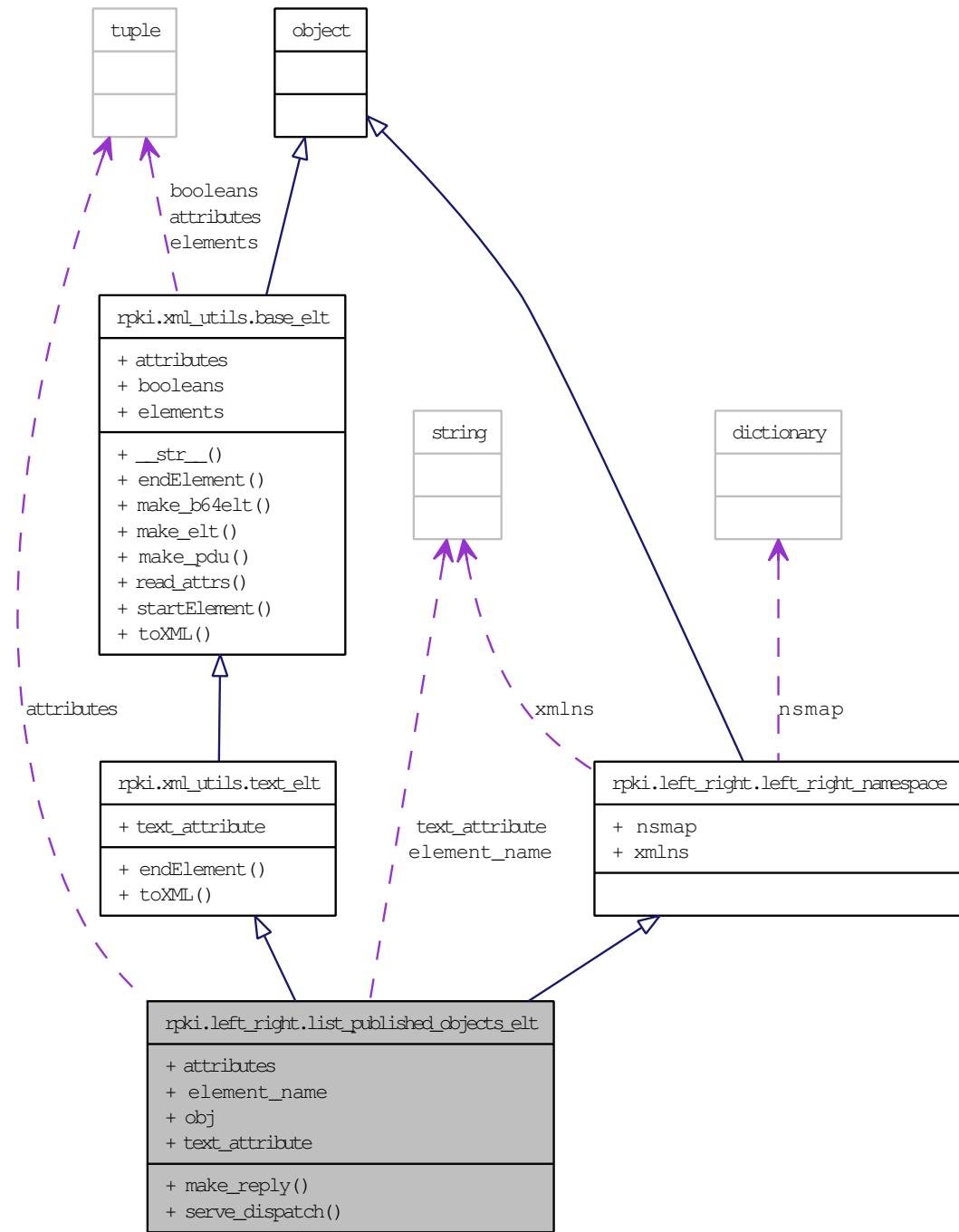
- [left_right.py \(3191\)](#)

10.118 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 rpk.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.

10.118.1 Detailed Description

<list_published_objects/> element.

Definition at line 968 of file left_right.py.

10.118.2 Member Function Documentation

10.118.2.1 def rpk.left_right.list_published_objects_elt.make_reply (*self, uri, obj*)

Generate one reply PDU.

Definition at line 995 of file left_right.py.

10.118.2.2 def rpk.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.

10.118.3 Member Data Documentation

10.118.3.1 tuple rpk.left_right.list_published_objects_elt.attributes = ("self_handle", "tag", "uri") [static]

XML attributes for this element.

Reimplemented from [rpk.xml_utils.base_elt](#).

Definition at line 974 of file left_right.py.

10.118.3.2 string rpk.left_right.list_published_objects_elt.element_name = "list_published_objects" [static]

Definition at line 973 of file left_right.py.

10.118.3.3 rpk.left_right.list_published_objects_elt.obj = None [static]

Definition at line 977 of file left_right.py.

10.118.3.4 string rpk.left_right.list_published_objects_elt.text_attribute = "obj" [static]

Name of the class attribute that holds the text value.

Reimplemented from [rpk.xml_utils.text_elt](#).

Definition at line 975 of file left_right.py.

The documentation for this class was generated from the following file:

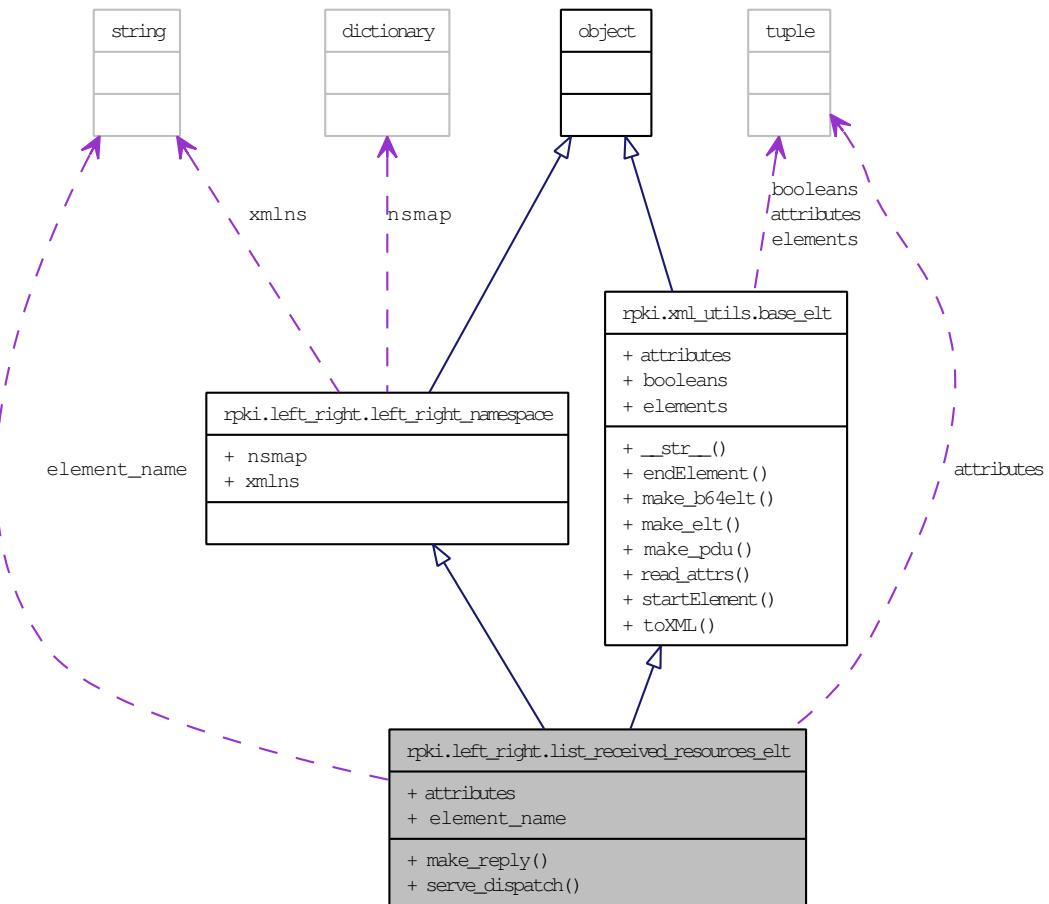
- [left_right.py \(3191\)](#)

10.119 rpk.left_right.list_received_resources_elt Class Reference

Inherits [rpk::xml_utils::base_elt](#), and [rpk::left_right::left_right_namespace](#).

Inherited by [irbe_cli.list_received_resources_elt](#).

Collaboration diagram for rpk.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"

10.119.1 Detailed Description

<list_received_resources/> element.

Definition at line 1003 of file left_right.py.

10.119.2 Member Function Documentation

10.119.2.1 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.

10.119.2.2 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.

10.119.3 Member Data Documentation

10.119.3.1 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.

**10.119.3.2 string rpki.left_right.list_received_resources_elt.element_name =
"list_received_resources" [static]**

Definition at line 1008 of file left_right.py.

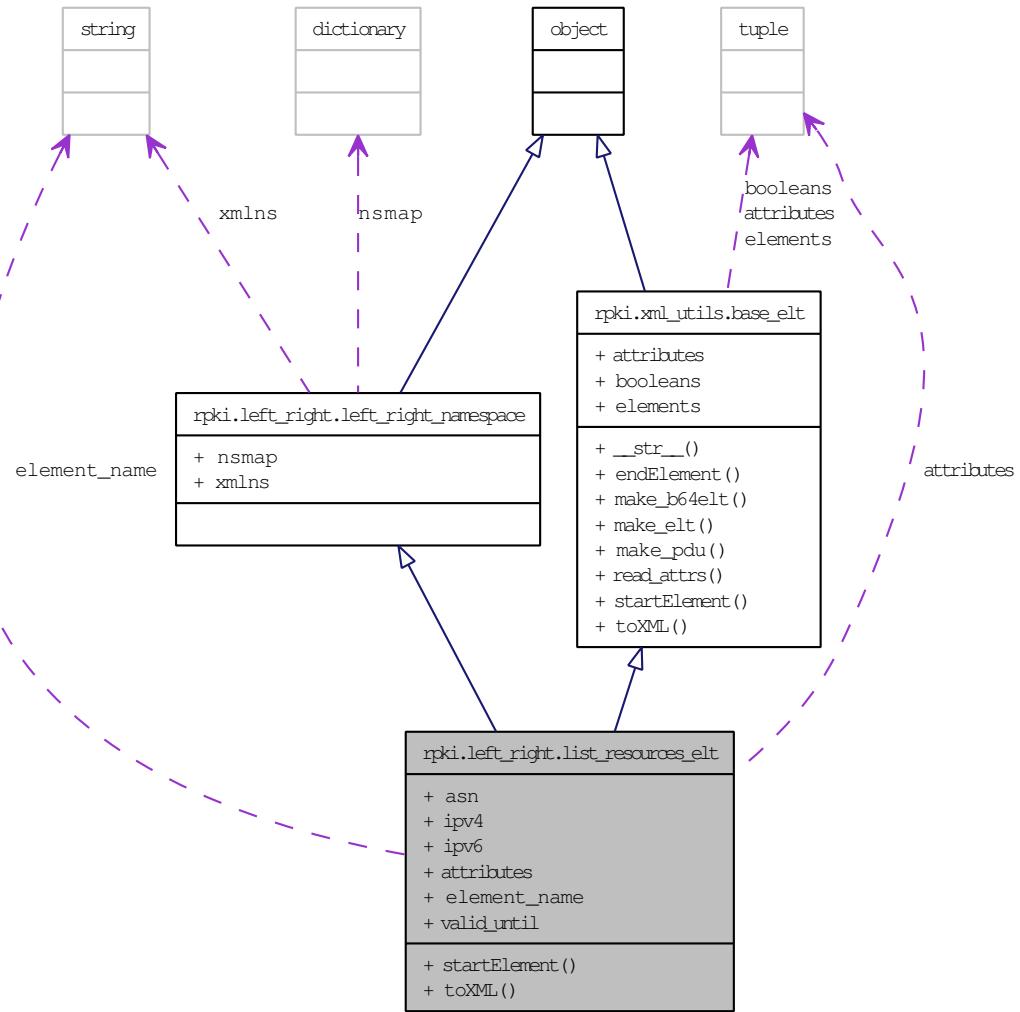
The documentation for this class was generated from the following file:

- [left_right.py \(3191\)](#)

10.120 rpki.left_right.list_resources_elt Class Reference

Inherits [rpki::xml_utils::base_elt](#), and [rpki::left_right::left_right_namespace](#).

Collaboration diagram for rpk.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

10.120.1 Detailed Description

<list_resources/> element.

Definition at line 913 of file left_right.py.

10.120.2 Member Function Documentation

10.120.2.1 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.

10.120.2.2 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.

10.120.3 Member Data Documentation**10.120.3.1 rpki.left_right.list_resources_elt.asn**

Definition at line 932 of file left_right.py.

```
10.120.3.2 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.

```
10.120.3.3 string rpki.left_right.list_resources_elt.element_name =
    "list_resources" [static]
```

Definition at line 918 of file left_right.py.

10.120.3.4 rpki.left_right.list_resources_elt.ipv4

Definition at line 934 of file left_right.py.

10.120.3.5 rpki.left_right.list_resources_elt.ipv6

Definition at line 936 of file left_right.py.

10.120.3.6 rpki.left_right.list_resources_elt.valid_until = None [static]

Definition at line 920 of file left_right.py.

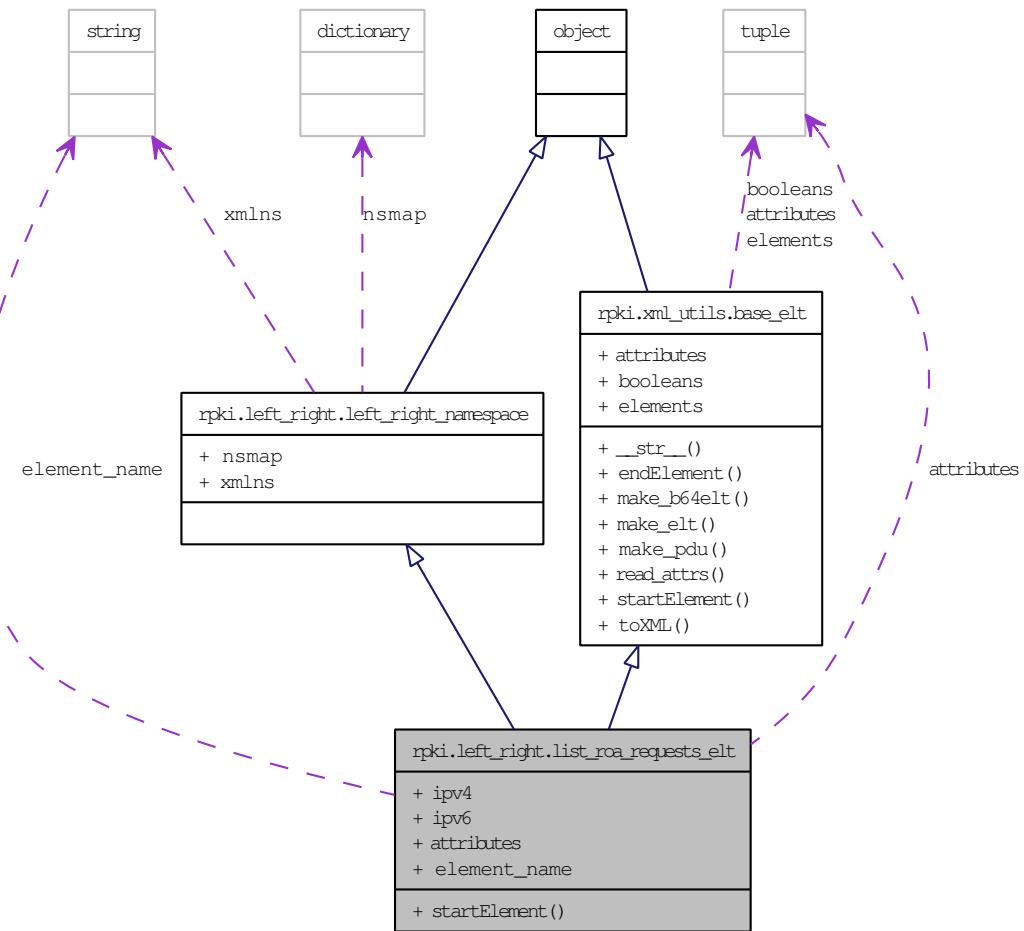
The documentation for this class was generated from the following file:

- [left_right.py \(3191\)](#)

10.121 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"

10.121.1 Detailed Description

<list_roa_requests/> element.

Definition at line 948 of file left_right.py.

10.121.2 Member Function Documentation

10.121.2.1 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.

10.121.3 Member Data Documentation

10.121.3.1 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.

10.121.3.2 string rpki.left_right.list_roa_requests_elt.element_name = "list_roa_requests" [static]

Definition at line 953 of file left_right.py.

10.121.3.3 rpki.left_right.list_roa_requests_elt.ipv4

Definition at line 964 of file left_right.py.

10.121.3.4 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:

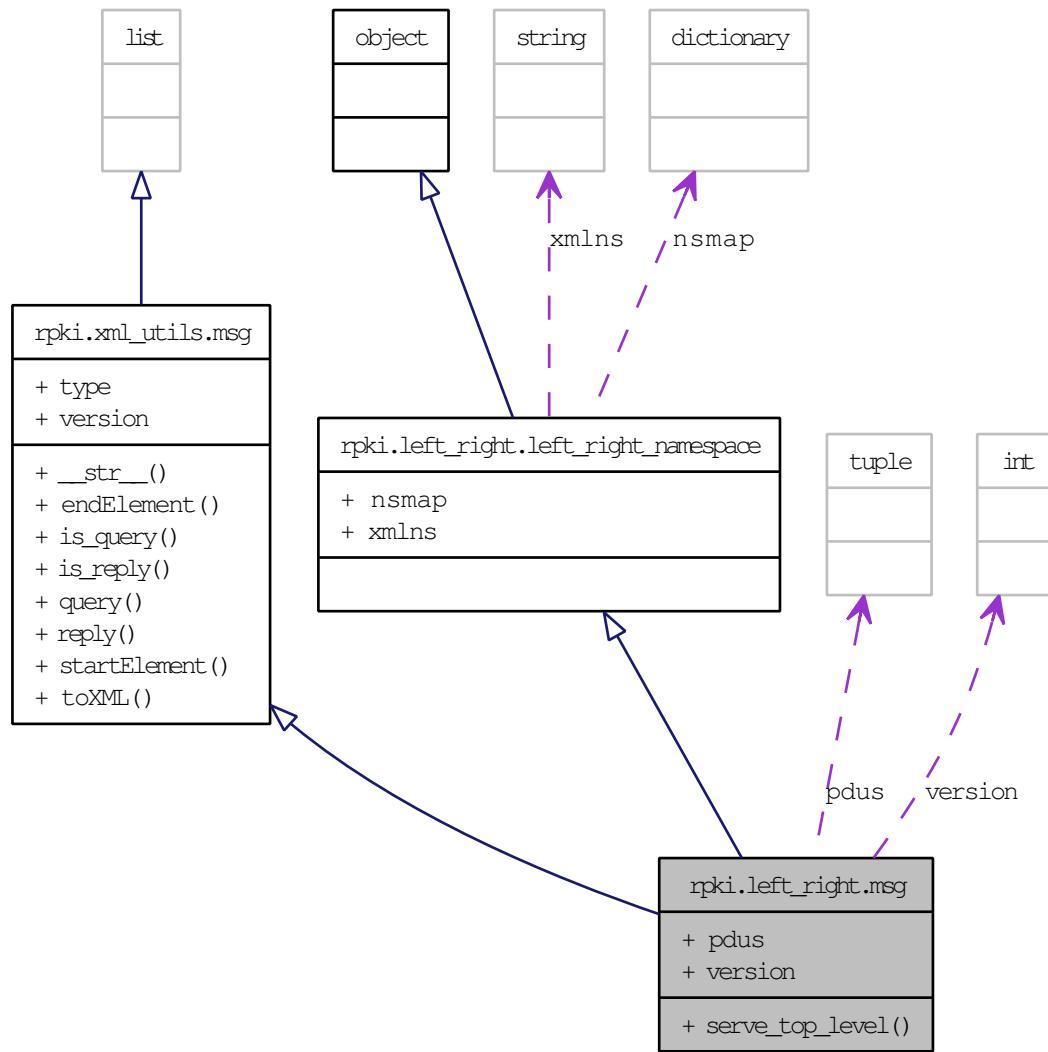
- [left_right.py \(3191\)](#)

10.122 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.

10.122.1 Detailed Description

Left-right PDU.

Definition at line 1066 of file left_right.py.

10.122.2 Member Function Documentation

10.122.2.1 def rpk.left_right.msg.serve_top_level (*self, gctx, cb*)

Serve one msg PDU.

Definition at line 1083 of file left_right.py.

10.122.3 Member Data Documentation

10.122.3.1 rpk::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.

10.122.3.2 rpk::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:

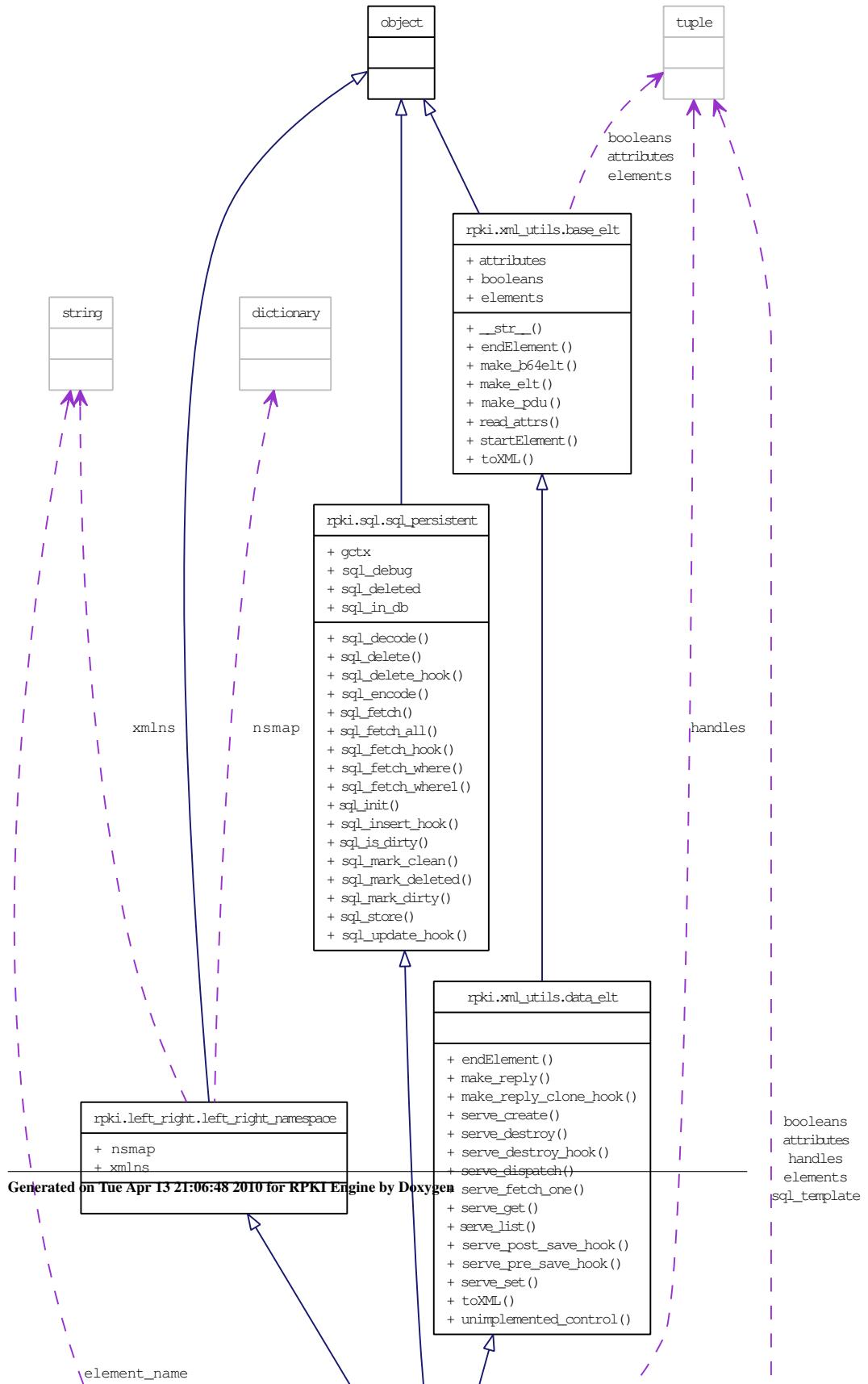
- [left_right.py \(3191\)](#)

10.123 rpk.left_right.parent_elt Class Reference

Inherits [rpki::left_right::data_elt](#).

Inherited by [irbe_cli.parent_elt](#).

Collaboration diagram for rpkic.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.
- `bpxi_cms_cert` = None
- `bpxi_cms_glue` = None
- `bpxi_https_cert` = None
- `bpxi_https_glue` = None
- string `element_name` = "parent"
- tuple `elements` = ("bpxi_cms_cert", "bpxi_cms_glue", "bpxi_https_cert", "bpxi_https_glue")
XML elements contained by this element.
- tuple `handles` = (("self", self_elt), ("bsc", bsc_elt), ("repository", repository_elt))
- tuple `sql_template`

10.123.1 Detailed Description

<parent/> element.

Definition at line 656 of file left_right.py.

10.123.2 Member Function Documentation

10.123.2.1 def rpk.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.

10.123.2.2 def rpk.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.

10.123.2.3 def rpk.left_right.parent_elt.repository (self)

Fetch repository object to which this parent object links.

Definition at line 679 of file left_right.py.

10.123.2.4 def rpk.left_right.parent_elt.serve_post_save_hook (self, q_pdu, r_pdu, cb, eb)

Extra server actions for parent_elt.

Reimplemented from [rpk.xml_utils.data_elt](#).

Definition at line 687 of file left_right.py.

10.123.2.5 def rpk.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.

10.123.2.6 def rpk.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.

10.123.2.7 def rpk.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.

10.123.3 Member Data Documentation**10.123.3.1 tuple rpk.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 [rpk.xml_utils.base_elt](#).

Definition at line 662 of file left_right.py.

**10.123.3.2 tuple rpk.left_right.parent_elt.booleans = ("rekey", "reissue",
"revoke", "revoke_forgotten") [static]**

Boolean attributes (value "yes" or "no") for this element.

Reimplemented from [rpk.xml_utils.base_elt](#).

Definition at line 665 of file left_right.py.

10.123.3.3 rpk.left_right.parent_elt.bpk_cms_cert = None [static]

Definition at line 674 of file left_right.py.

10.123.3.4 rpki.left_right.parent_elt.bpkı_cms_glue = None [static]

Definition at line 675 of file left_right.py.

10.123.3.5 rpki.left_right.parent_elt.bpkı_https_cert = None [static]

Definition at line 676 of file left_right.py.

10.123.3.6 rpki.left_right.parent_elt.bpkı_https_glue = None [static]

Definition at line 677 of file left_right.py.

10.123.3.7 string rpki.left_right.parent_elt.element_name = "parent" [static]

Definition at line 661 of file left_right.py.

10.123.3.8 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.

10.123.3.9 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.

10.123.3.10 tuple rpk.left_right.parent_elt.sql_template [static]**Initial value:**

```
rpk.sql.template("parent", "parent_id", "parent_handle",
                  "self_id", "bsc_id", "repository_id",
                  ("bpki_cms_cert", rpk.x509.X509), ("bpki_cms_
glue", rpk.x509.X509),
                  ("bpki_https_cert", rpk.x509.X509), ("bpki_ht
tps_glue", rpk.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:

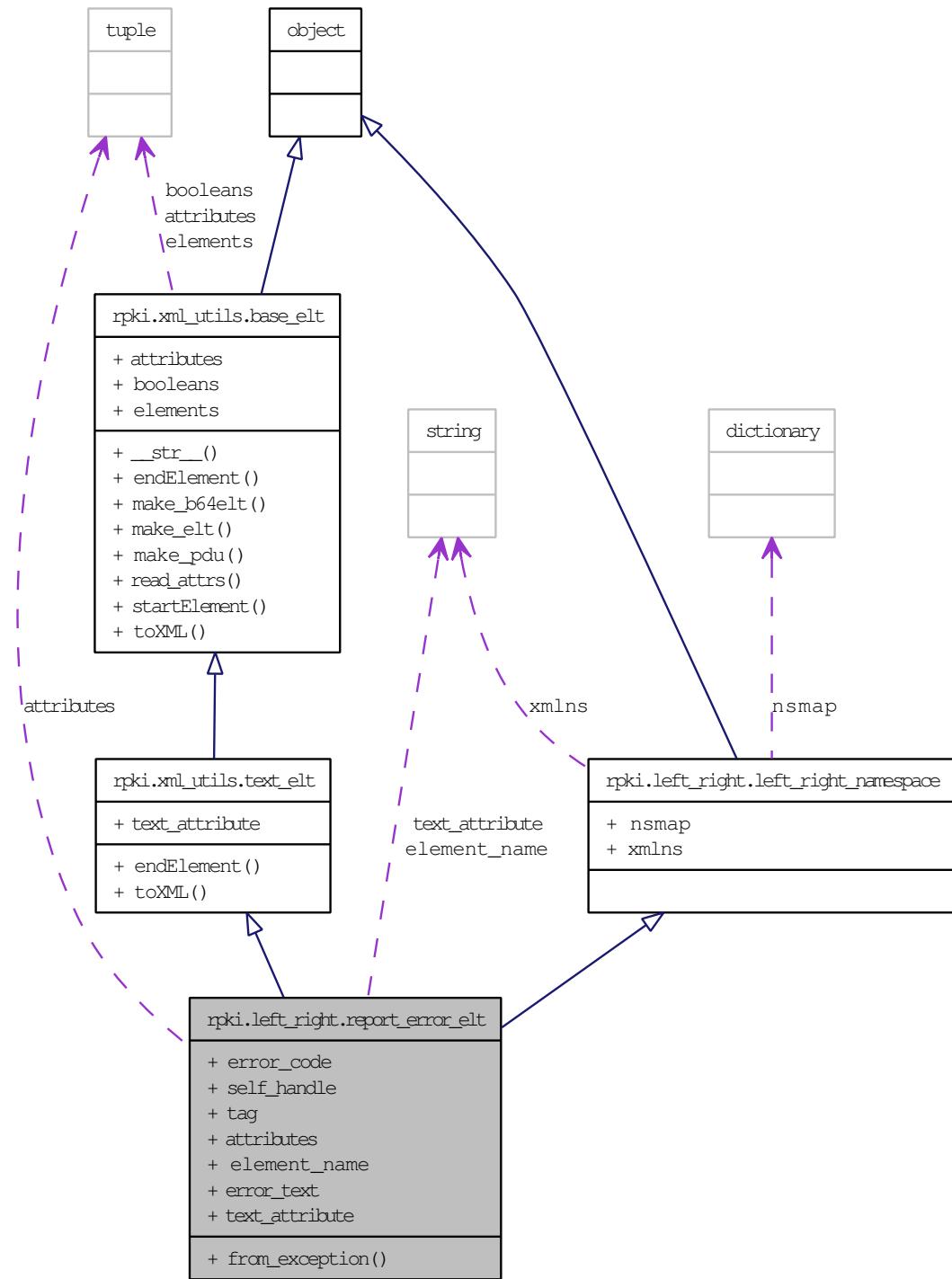
- [left_right.py \(3191\)](#)

10.124 rpk.left_right.report_error_elt Class Reference

Inherits [rpk::xml_utils::text_elt](#), and [rpk::left_right::left_right_namespace](#).

Inherited by [irbe_cli.report_error_elt](#).

Collaboration diagram for rpk.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.

10.124.1 Detailed Description

<report_error/> element.

Definition at line 1043 of file left_right.py.

10.124.2 Member Function Documentation

10.124.2.1 def rpk.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.

10.124.3 Member Data Documentation

10.124.3.1 tuple rpk.left_right.report_error_elt.attributes = ("tag", "self_handle", "error_code") [static]

XML attributes for this element.

Reimplemented from [rpk.xml_utils.base_elt](#).

Definition at line 1049 of file left_right.py.

10.124.3.2 string rpk.left_right.report_error_elt.element_name = "report_error" [static]

Definition at line 1048 of file left_right.py.

10.124.3.3 rpk.left_right.report_error_elt.error_code

Definition at line 1062 of file left_right.py.

10.124.3.4 rpk.left_right.report_error_elt.error_text = None [static]

Definition at line 1052 of file left_right.py.

10.124.3.5 rpk.left_right.report_error_elt.self_handle

Definition at line 1060 of file left_right.py.

10.124.3.6 rpk.left_right.report_error_elt.tag

Definition at line 1061 of file left_right.py.

**10.124.3.7 string rpkি.left_right.report_error_elt.text_attribute = "error_text"
[static]**

Name of the class attribute that holds the text value.

Reimplemented from [rpkি.xml_utils.text_elt](#).

Definition at line 1050 of file left_right.py.

The documentation for this class was generated from the following file:

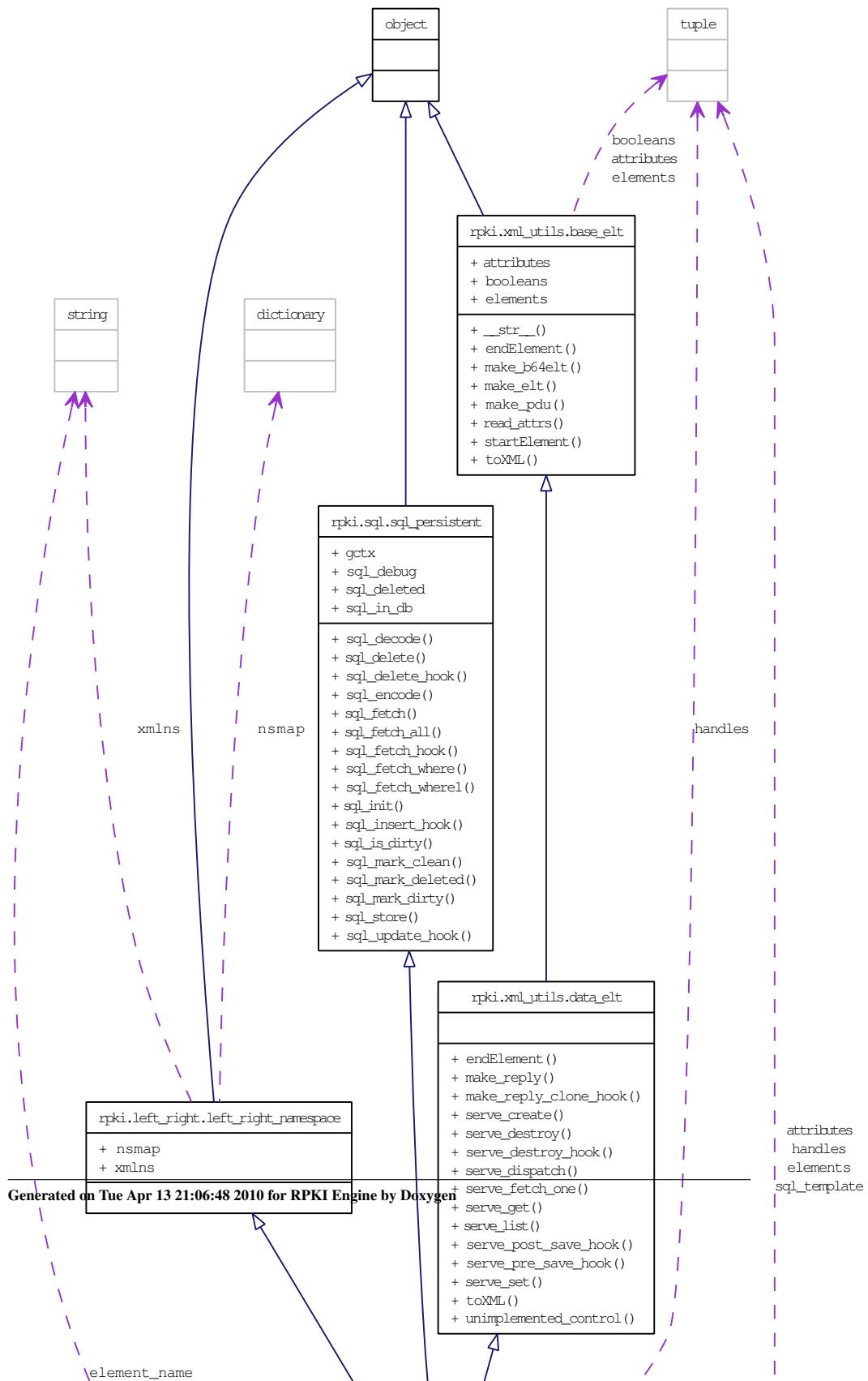
- [left_right.py \(3191\)](#)

10.125 rpkি.left_right.repository_elt Class Reference

Inherits [rpkি::left_right::data_elt](#).

Inherited by [irbe_cli.repository_elt](#).

Collaboration diagram for rpk.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.

- `bpxi_cert` = None
- `bpxi_glue` = None
- string `element_name` = "repository"
- tuple `elements` = ("bpxi_cert", "bpxi_glue")

XML elements contained by this element.

- tuple `handles` = ((`"self"`, `self_elt`), (`"bsc"`, `bsc_elt`))
- tuple `sql_template`

10.125.1 Detailed Description

`<repository/>` element.

Definition at line 573 of file left_right.py.

10.125.2 Member Function Documentation

10.125.2.1 def rpk.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.

10.125.2.2 def rpk.left_right.repository_elt.default_pubd_handler (*pdu*)

Default handler for publication response PDUs.

Definition at line 595 of file left_right.py.

10.125.2.3 def rpk.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.

10.125.3 Member Data Documentation**10.125.3.1 tuple rpk.left_right.repository_elt.attributes = ("action", "tag", "self_handle", "repository_handle", "bsc_handle", "peer_contact_uri") [static]**

XML attributes for this element.

Reimplemented from [rpk.xml_utils.base_elt](#).

Definition at line 579 of file left_right.py.

10.125.3.2 rpk.left_right.repository_elt.bpk.cert = None [static]

Definition at line 587 of file left_right.py.

10.125.3.3 rpk.left_right.repository_elt.bpk.glue = None [static]

Definition at line 588 of file left_right.py.

10.125.3.4 string rpk.left_right.repository_elt.element_name = "repository" [static]

Definition at line 578 of file left_right.py.

10.125.3.5 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.

10.125.3.6 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.

10.125.3.7 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:

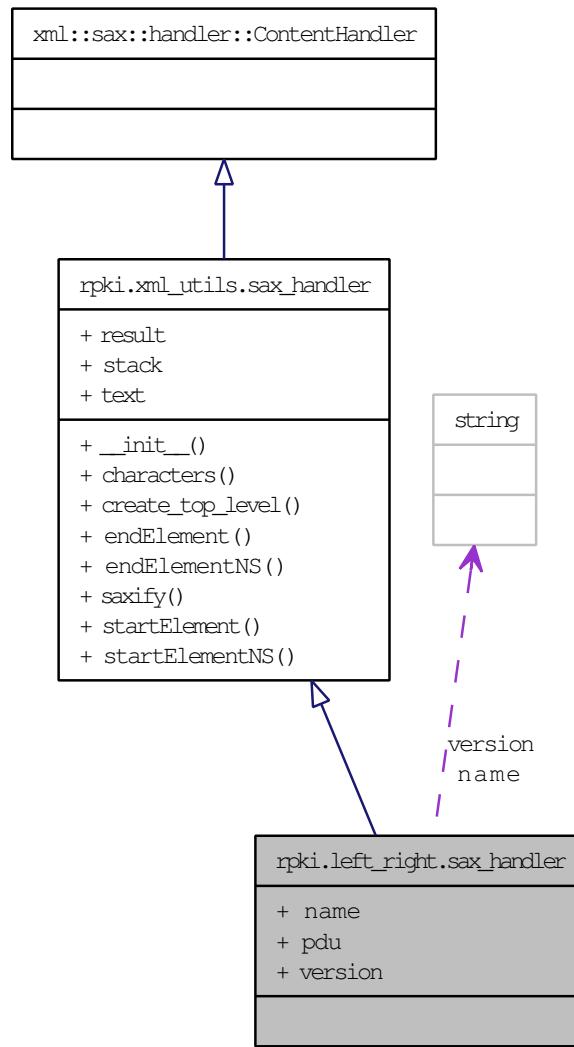
- [left_right.py \(3191\)](#)

10.126 rpki.left_right.sax_handler Class Reference

Inherits [rpki::xml_utils::sax_handler](#).

Inherited by [irbe_cli.left_right_sax_handler](#).

Collaboration diagram for rpk.left_right.sax_handler:



Static Public Attributes

- string `name` = "msg"
- `pdu` = `msg`
- string `version` = "1"

10.126.1 Detailed Description

SAX handler for Left-Right protocol.

Definition at line 1111 of file `left_right.py`.

10.126.2 Member Data Documentation

10.126.2.1 `string rpkி.left_right.sax_handler.name = "msg" [static]`

Definition at line 1117 of file `left_right.py`.

10.126.2.2 `rpkி.left_right.sax_handler.pdu = msg [static]`

Reimplemented in [irbe_cli.left_right.sax_handler](#).

Definition at line 1116 of file `left_right.py`.

10.126.2.3 `string rpkி.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:

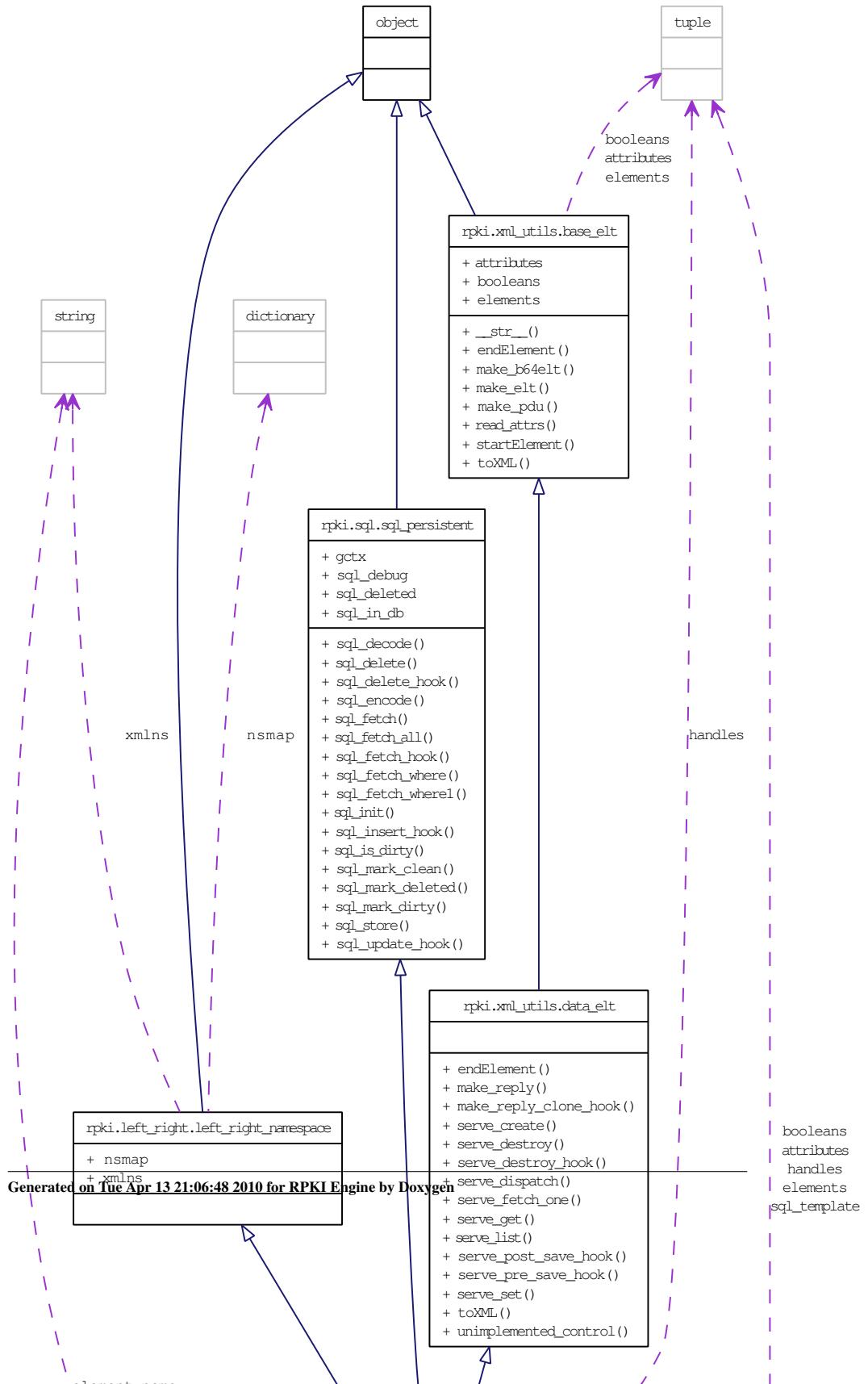
- [left_right.py \(3191\)](#)

10.127 `rpkி.left_right.self_elt` Class Reference

Inherits [rpkி::left_right::data_elt](#).

Inherited by [irbe_cli.self_elt](#).

Collaboration diagram for rpkic.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.

- `bpxi_cert` = None
- `bpxi_glue` = None
- `crl_interval` = None
- string `element_name` = "self"
- tuple `elements` = ("bpxi_cert", "bpxi_glue")

XML elements contained by this element.

- tuple `handles` = ()
- `regen_margin` = None
- tuple `sql_template`
- `use_hsm` = False

10.127.1 Detailed Description

<self/> element.

Definition at line 124 of file left_right.py.

10.127.2 Member Function Documentation

10.127.2.1 def rpk.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.

10.127.2.2 def rpk.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.

10.127.2.3 def rpk.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.

10.127.2.4 def rpk.left_right.self_elt.cron (*self, cb*)

Periodic tasks.

Definition at line 274 of file left_right.py.

10.127.2.5 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.

10.127.2.6 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.

10.127.2.7 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.

10.127.2.8 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.

10.127.2.9 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.

10.127.2.10 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.

10.127.2.11 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.

10.127.2.12 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.

10.127.2.13 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.

10.127.2.14 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.

10.127.2.15 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.

10.127.2.16 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.

10.127.2.17 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.

10.127.2.18 def rpkি.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.

10.127.2.19 def rpkি.left_right.self_elt.update_roas (self, cb)

Generate or update ROAs for this `self`.

Definition at line 470 of file left_right.py.

10.127.3 Member Data Documentation**10.127.3.1 tuple rpkি.left_right.self_elt.attributes = ("action", "tag", "self_handle", "crl_interval", "regen_margin") [static]**

XML attributes for this element.

Reimplemented from [rpkি.xml_utils.base_elt](#).

Definition at line 130 of file left_right.py.

10.127.3.2 tuple rpkি.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 [rpkি.xml_utils.base_elt](#).

Definition at line 132 of file left_right.py.

10.127.3.3 rpkি.left_right.self_elt.bpkি_cert = None [static]

Definition at line 142 of file left_right.py.

10.127.3.4 rpki.left_right.self_elt.bpkiglue = None [static]

Definition at line 143 of file left_right.py.

10.127.3.5 rpki.left_right.self_elt.crl_interval = None [static]

Definition at line 140 of file left_right.py.

10.127.3.6 string rpki.left_right.self_elt.element_name = "self" [static]

Definition at line 129 of file left_right.py.

10.127.3.7 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.

10.127.3.8 tuple rpki.left_right.self_elt.handles = () [static]

Reimplemented from [rpki.left_right.data_elt](#).

Definition at line 137 of file left_right.py.

10.127.3.9 rpki.left_right.self_elt.regen_margin = None [static]

Definition at line 141 of file left_right.py.

10.127.3.10 tuple rpki.left_right.self_elt.sql_template [static]

Initial value:

```
rpkilog.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.

10.127.3.11 rpkilog.left_right.self_elt.use_hsm = False [static]

Definition at line 139 of file left_right.py.

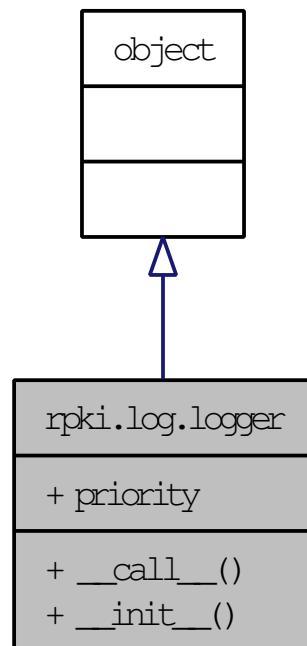
The documentation for this class was generated from the following file:

- [left_right.py \(3191\)](#)

10.128 rpkilog.logger Class Reference

Inherits [object](#).

Collaboration diagram for rpkilog.logger:



Public Member Functions

- def [__call__](#)
- def [__init__](#)

Public Attributes

- [priority](#)

10.128.1 Detailed Description

Closure for logging.

Definition at line 71 of file log.py.

10.128.2 Member Function Documentation

10.128.2.1 def rpkilogger.__call__ (*self, message*)

Definition at line 79 of file log.py.

10.128.2.2 def rpkilogger.__init__ (*self, priority*)

Definition at line 76 of file log.py.

10.128.3 Member Data Documentation

10.128.3.1 rpkilogger.priority

Definition at line 77 of file log.py.

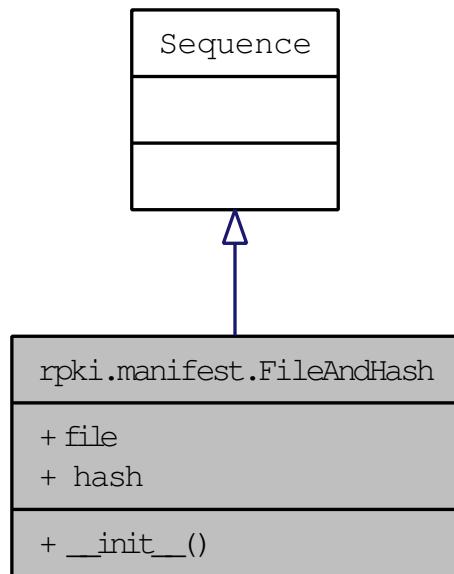
The documentation for this class was generated from the following file:

- [log.py \(3107\)](#)

10.129 rpkimaniifest.FileAndHash Class Reference

Inherits [Sequence](#).

Collaboration diagram for rpkimaniifest.FileAndHash:



Public Member Functions

- def [__init__](#)

Public Attributes

- [file](#)
- [hash](#)

10.129.1 Detailed Description

Definition at line 27 of file manifest.py.

10.129.2 Member Function Documentation**10.129.2.1 def rpki.manifest.FileAndHash.__init__ (*self*, *optional* = 0, *default* = ")**

Definition at line 28 of file manifest.py.

10.129.3 Member Data Documentation**10.129.3.1 rpki.manifest.FileAndHash.file**

Definition at line 29 of file manifest.py.

10.129.3.2 rpki.manifest.FileAndHash.hash

Definition at line 30 of file manifest.py.

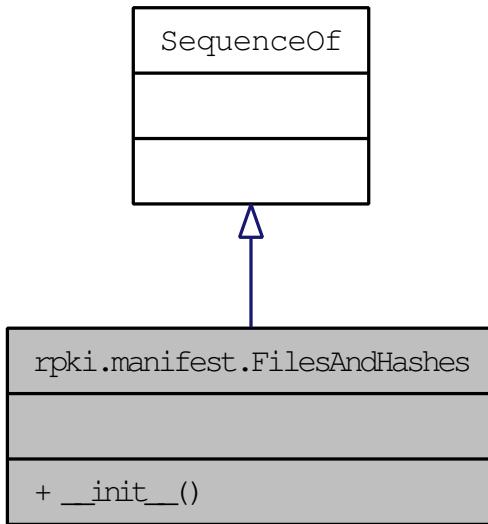
The documentation for this class was generated from the following file:

- [manifest.py \(2424\)](#)

10.130 rpki.manifest.FilesAndHashes Class Reference

Inherits [SequenceOf](#).

Collaboration diagram for rpkি.manifest.FilesAndHashes:



Public Member Functions

- def [__init__](#)

10.130.1 Detailed Description

Definition at line 34 of file manifest.py.

10.130.2 Member Function Documentation

10.130.2.1 def rpkি.manifest.FilesAndHashes.__init__ (*self*, *optional* = 0, *default* = "")

Definition at line 35 of file manifest.py.

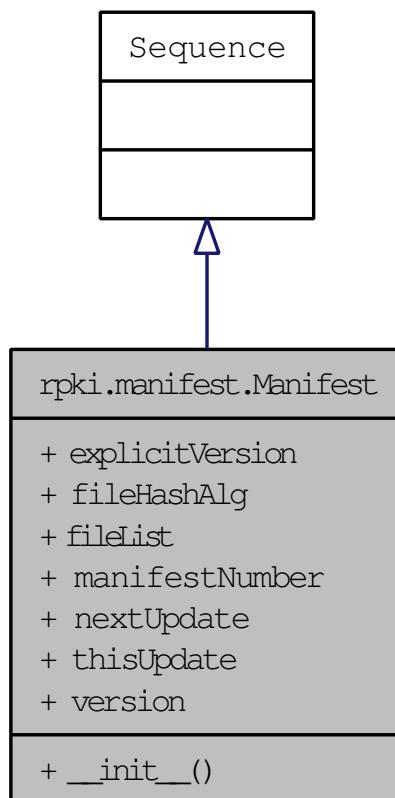
The documentation for this class was generated from the following file:

- [manifest.py \(2424\)](#)

10.131 rpkি.manifest.Manifest Class Reference

Inherits [Sequence](#).

Collaboration diagram for rpkি.manifest.Manifest:



Public Member Functions

- def [__init__](#)

Public Attributes

- [explicitVersion](#)
- [fileHashAlg](#)
- [fileList](#)
- [manifestNumber](#)
- [nextUpdate](#)

- [thisUpdate](#)
- [version](#)

10.131.1 Detailed Description

Definition at line 38 of file manifest.py.

10.131.2 Member Function Documentation

10.131.2.1 def rpkি.manifest.Manifest.__init__ (*self*, *optional* = 0, *default* = "")

Definition at line 39 of file manifest.py.

10.131.3 Member Data Documentation

10.131.3.1 rpkি.manifest.Manifest.explicitVersion

Definition at line 41 of file manifest.py.

10.131.3.2 rpkি.manifest.Manifest.fileHashAlg

Definition at line 45 of file manifest.py.

10.131.3.3 rpkি.manifest.Manifest fileList

Definition at line 46 of file manifest.py.

10.131.3.4 rpkি.manifest.Manifest.manifestNumber

Definition at line 42 of file manifest.py.

10.131.3.5 rpki.manifest.Manifest.nextUpdate

Definition at line 44 of file manifest.py.

10.131.3.6 rpki.manifest.Manifest.thisUpdate

Definition at line 43 of file manifest.py.

10.131.3.7 rpki.manifest.Manifest.version

Definition at line 40 of file manifest.py.

The documentation for this class was generated from the following file:

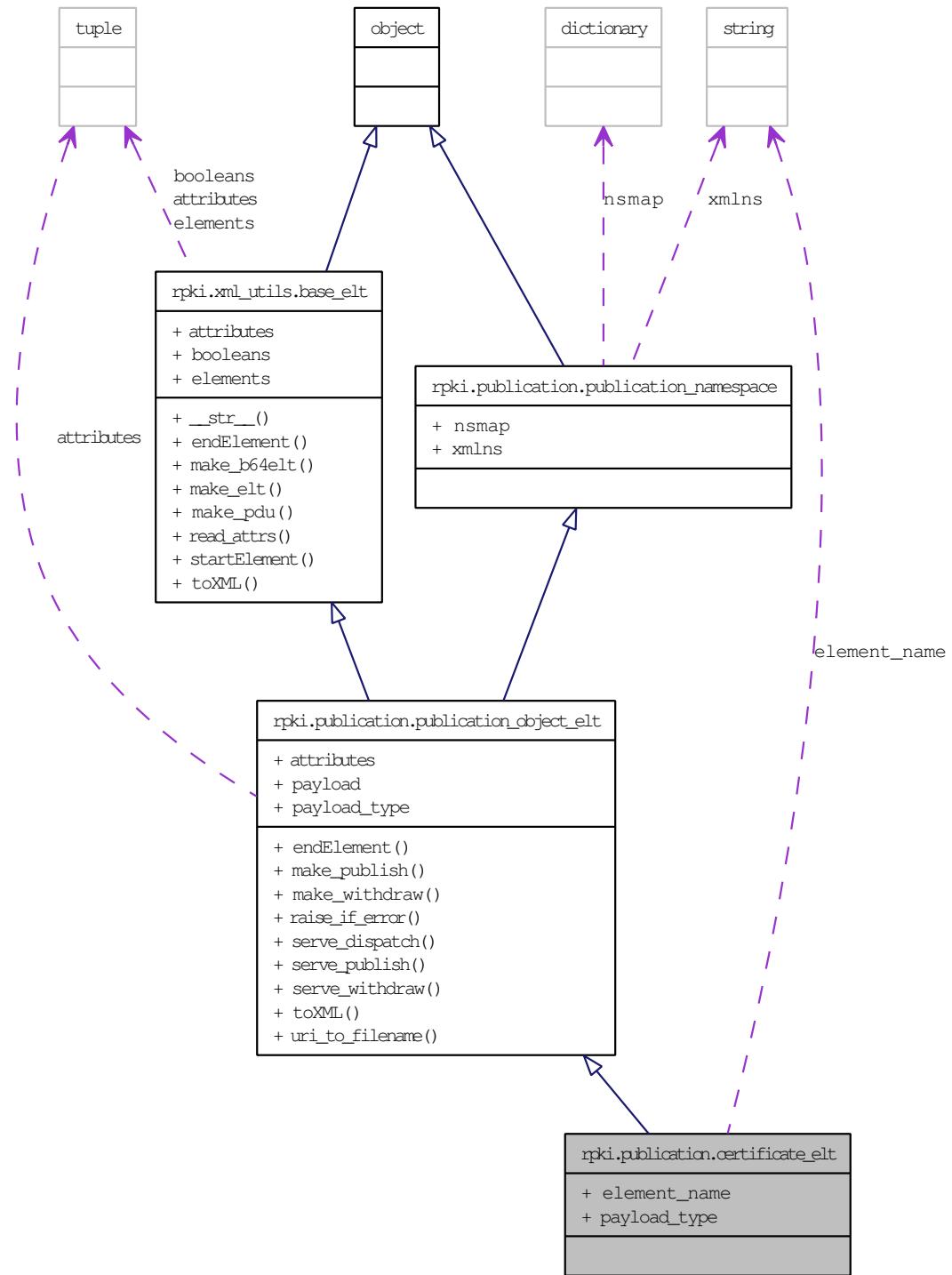
- [manifest.py \(2424\)](#)

10.132 rpki.publication.certificate_elt Class Reference

Inherits [rpki::publication::publication_object_elt](#).

Inherited by [irbe_cli.certificate_elt](#).

Collaboration diagram for rpkি.publication.certificate_elt:



Static Public Attributes

- string `element_name` = "certificate"
- `payload_type` = [rpk.x509.X509](#)

10.132.1 Detailed Description

`<certificate/>` element.

Definition at line 287 of file publication.py.

10.132.2 Member Data Documentation**10.132.2.1 string rpk.publication.certificate_elt.element_name = "certificate"
[static]**

Definition at line 292 of file publication.py.

**10.132.2.2 rpk.publication.certificate_elt.payload_type = rpk.x509.X509
[static]**

Reimplemented from [rpk.publication.publication_object_elt](#).

Definition at line 293 of file publication.py.

The documentation for this class was generated from the following file:

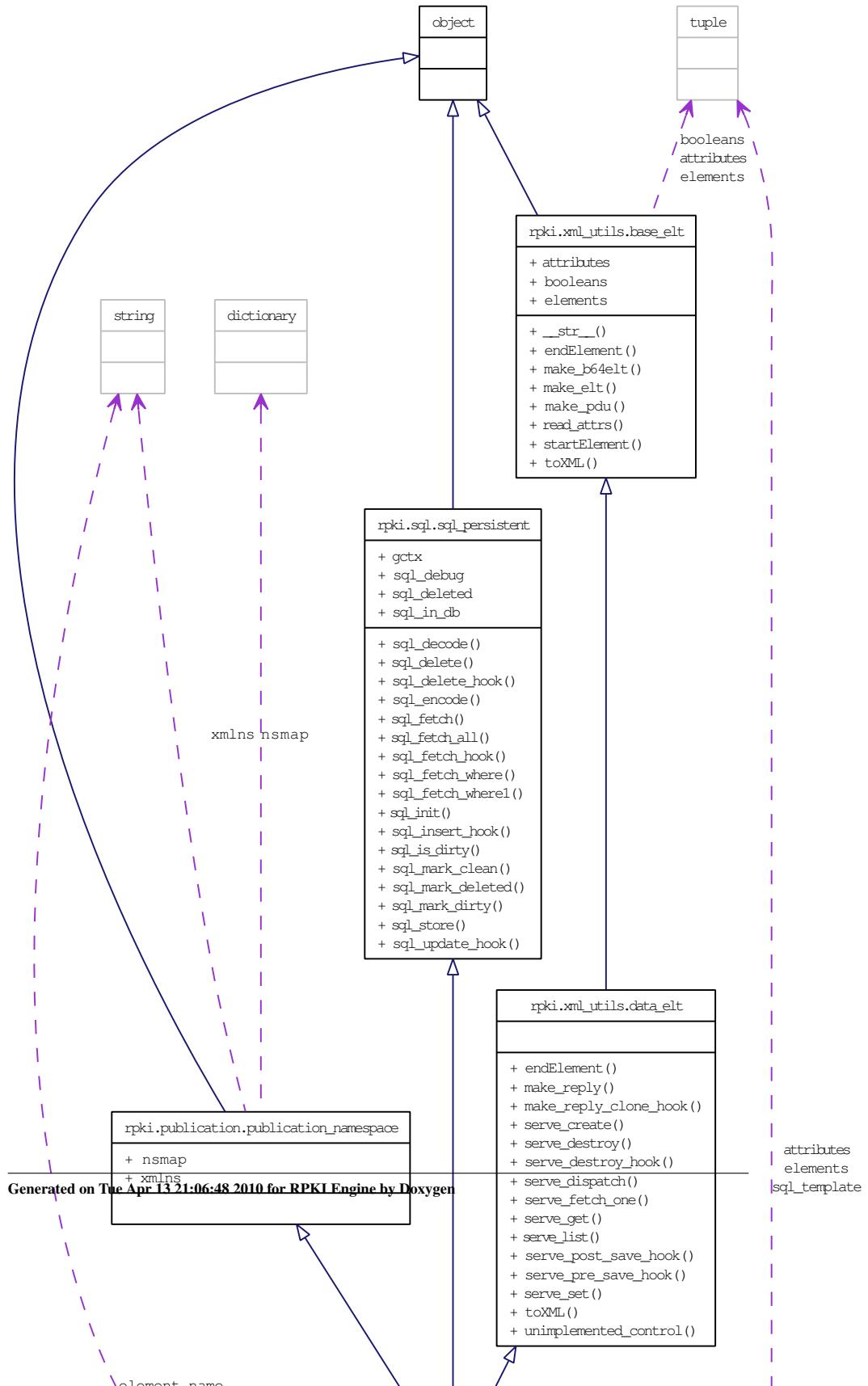
- [publication.py \(3107\)](#)

10.133 rpk.publication.client_elt Class Reference

Inherits [rpk::publication::control_elt](#).

Inherited by [irbe_cli.client_elt](#).

Collaboration diagram for rpkি.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
- `bpxi_cert` = None
- `bpxi_glue` = None
- `clear_https_ta_cache` = False
- string `element_name` = "client"
- tuple `elements` = ("bpxi_cert", "**bpxi_glue**")
XML elements contained by this element.
- tuple `sql_template` = `rpxi.sql.template("client", "client_id", "client_handle", "base_uri", ("bpxi_cert", rpxi.x509.X509), ("bpxi_glue", rpxi.x509.X509))`

10.133.1 Detailed Description

<client/> element.

Definition at line 113 of file publication.py.

10.133.2 Member Function Documentation

10.133.2.1 def rpki.publication.client_elt.check_allowed_uri (*self*, *uri*)

Definition at line 160 of file publication.py.

10.133.2.2 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.

10.133.2.3 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.

10.133.2.4 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.

10.133.2.5 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.

10.133.3 Member Data Documentation

10.133.3.1 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.

10.133.3.2 rpki.publication.client_elt.base_uri = None [static]

Definition at line 124 of file publication.py.

10.133.3.3 rpki.publication.client_elt.bpkı_cert = None [static]

Definition at line 125 of file publication.py.

10.133.3.4 rpki.publication.client_elt.bpkı_glue = None [static]

Definition at line 126 of file publication.py.

10.133.3.5 rpki.publication.client_elt.clear_https_ta_cache = False [static]

Definition at line 128 of file publication.py.

10.133.3.6 string rpki.publication.client_elt.element_name = "client" [static]

Definition at line 118 of file publication.py.

10.133.3.7 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.

```
10.133.3.8 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:

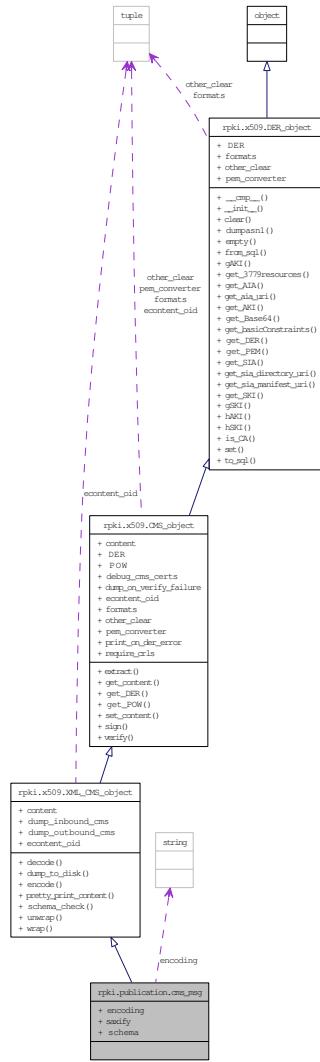
- [publication.py \(3107\)](#)

10.134 rpki.publication.cms_msg Class Reference

Inherits [rpki::x509::XML_CMS_object](#).

Inherited by [irbe_cli.publication_cms_msg](#).

Collaboration diagram for rpkি.publication.cms_msg:



Static Public Attributes

- `string encoding = "us-ascii"`
- `saxify = sax_handler.saxify`
- `schema = rpkি.relaxng.publication`

10.134.1 Detailed Description

Class to hold a CMS-signed publication PDU.

Definition at line 415 of file publication.py.

10.134.2 Member Data Documentation

10.134.2.1 string rpki.publication.cms_msg.encoding = "us-ascii" [static]

Definition at line 420 of file publication.py.

10.134.2.2 rpki.publication.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented in [irbe_cli.publication_cms_msg](#).

Definition at line 422 of file publication.py.

10.134.2.3 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:

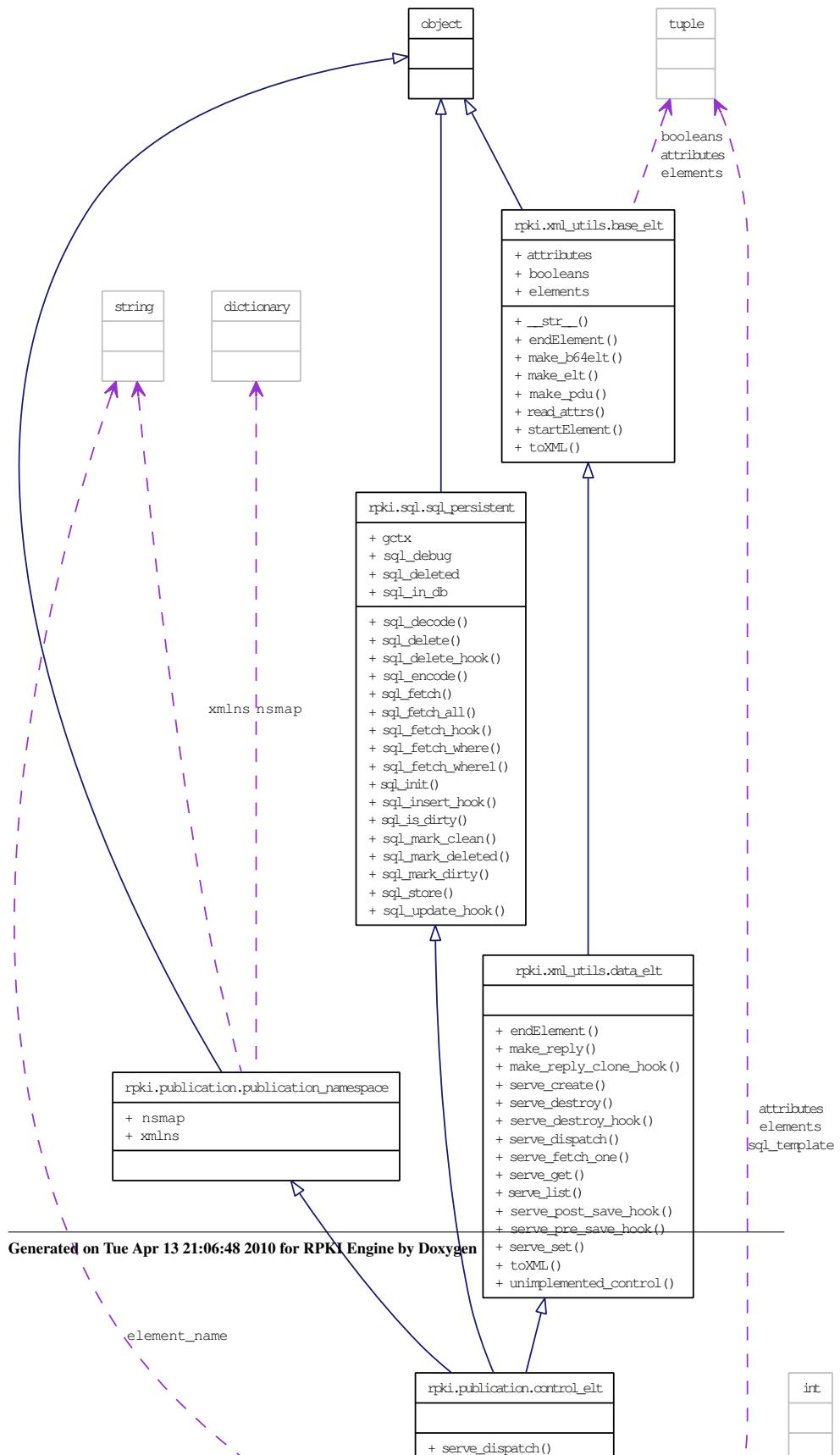
- [publication.py \(3107\)](#)

10.135 rpki.publication.config_elt Class Reference

Inherits [rpki::publication::control_elt](#).

Inherited by [irbe_cli.config_elt](#).

Collaboration diagram for rpkি.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` = `rpk.sql.template("config", "config_id", ("bpki_crl", rpk.x509.CRL))`
- int `wired_in_config_id` = 1

10.135.1 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.

10.135.2 Member Function Documentation

10.135.2.1 def rpk.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.

10.135.2.2 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.

10.135.2.3 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.

10.135.2.4 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.

10.135.3 Member Data Documentation**10.135.3.1 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.

10.135.3.2 rpki.publication.config_elt.config_id

Definition at line 86 of file publication.py.

**10.135.3.3 string rpki.publication.config_elt.element_name = "config"
[static]**

Definition at line 73 of file publication.py.

**10.135.3.4 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.

**10.135.3.5 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.

10.135.3.6 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:

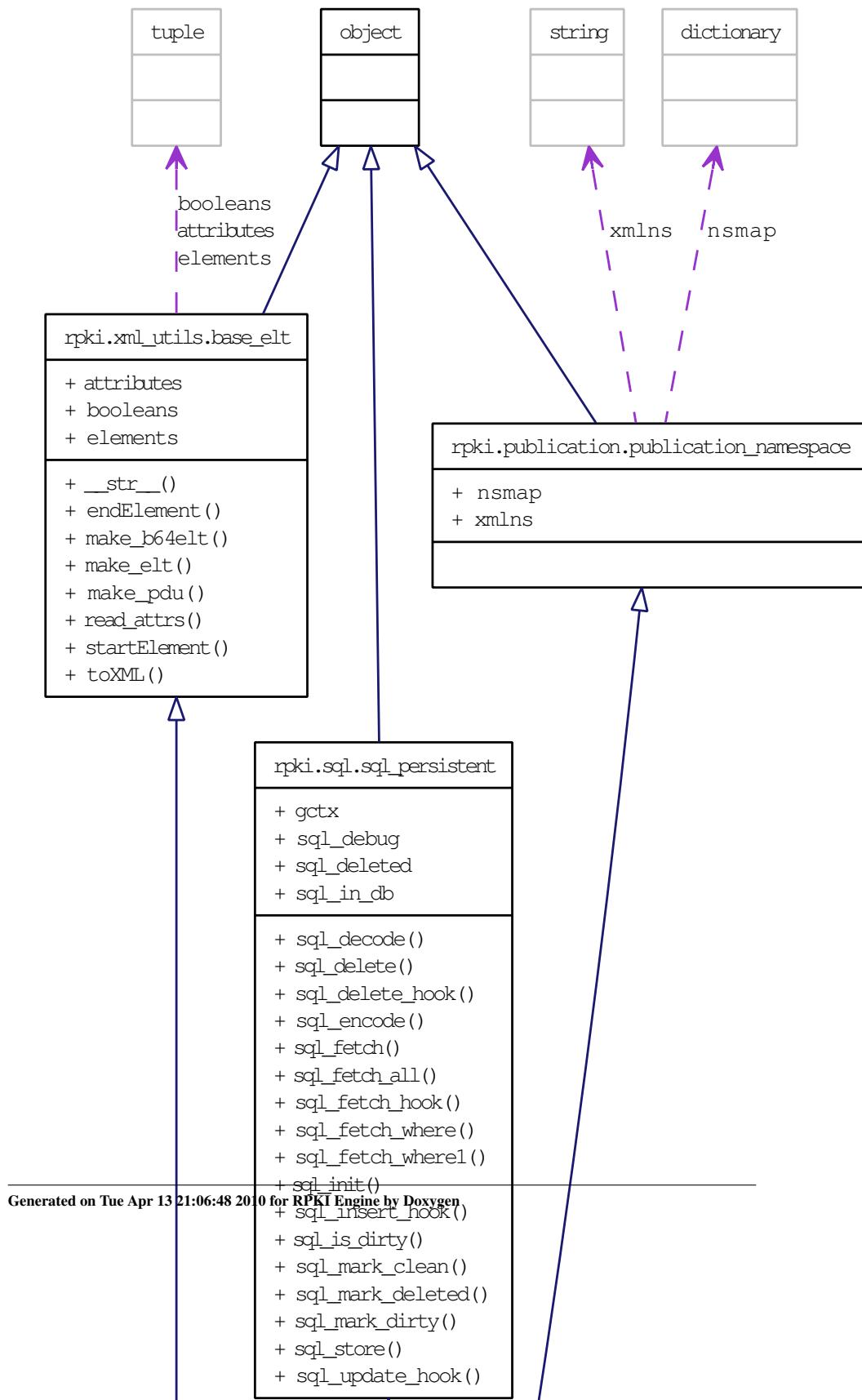
- [publication.py \(3107\)](#)

10.136 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 rpkি.publication.control_elt:



Public Member Functions

- def [serve_dispatch](#)

10.136.1 Detailed Description

Virtual class for control channel objects.

Definition at line 47 of file publication.py.

10.136.2 Member Function Documentation

10.136.2.1 def rpk.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 [rpk.xml_utils.data_elt](#).

Definition at line 52 of file publication.py.

The documentation for this class was generated from the following file:

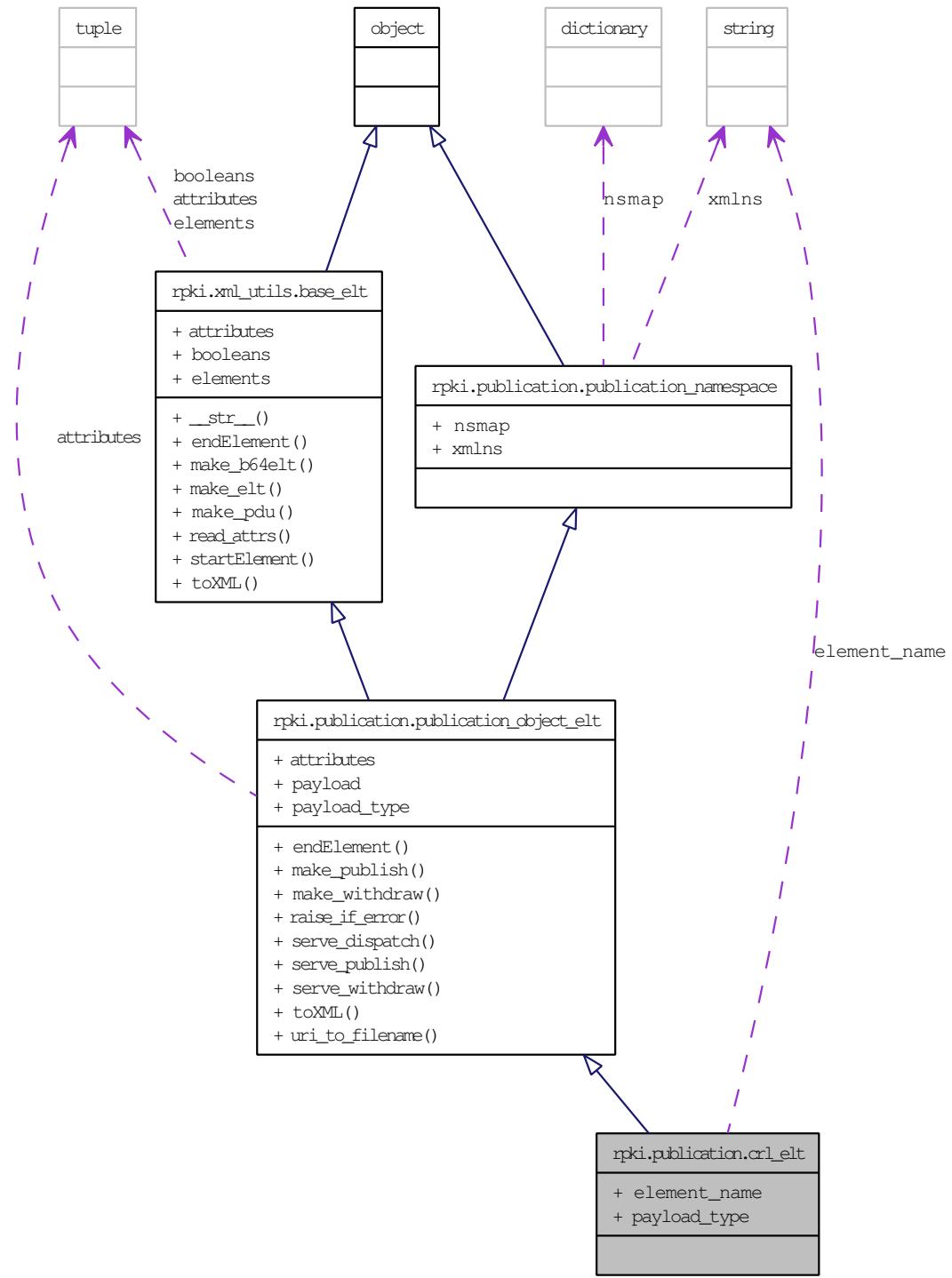
- [publication.py \(3107\)](#)

10.137 rpk.publication.crl_elt Class Reference

Inherits [rpk::publication::publication_object_elt](#).

Inherited by [irbe_cli.crl_elt](#).

Collaboration diagram for rpkি.publication.crl_elt:



Static Public Attributes

- string `element_name` = "crl"
- `payload_type` = `rpk.x509.CRL`

10.137.1 Detailed Description

`<crl/> element.`

Definition at line 295 of file publication.py.

10.137.2 Member Data Documentation

10.137.2.1 string `rpk.publication.crl_elt.element_name` = "crl" [static]

Definition at line 300 of file publication.py.

10.137.2.2 `rpk.publication.crl_elt.payload_type` = `rpk.x509.CRL` [static]

Reimplemented from `rpk.publication.publication_object_elt`.

Definition at line 301 of file publication.py.

The documentation for this class was generated from the following file:

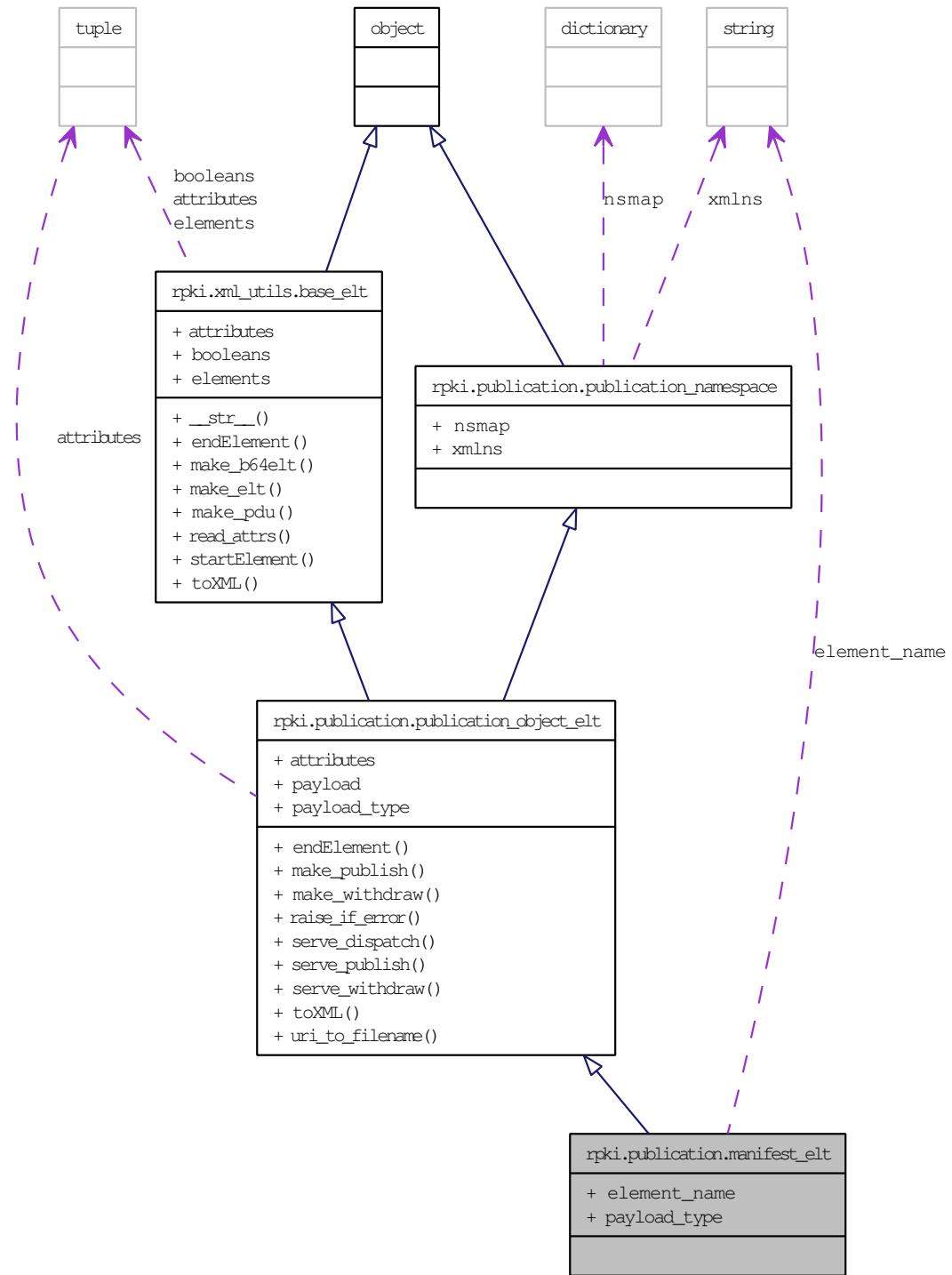
- `publication.py` (3107)

10.138 rpk.publication.manifest_elt Class Reference

Inherits `rpk::publication::publication_object_elt`.

Inherited by `irbe_cli.manifest_elt`.

Collaboration diagram for rpkি.publication.manifest_elt:



Static Public Attributes

- string `element_name` = "manifest"
- `payload_type` = `rpk.x509.SignedManifest`

10.138.1 Detailed Description

<manifest/> element.

Definition at line 303 of file publication.py.

10.138.2 Member Data Documentation

10.138.2.1 string rpk.publication.manifest_elt.element_name = "manifest" [static]

Definition at line 308 of file publication.py.

10.138.2.2 rpk.publication.manifest_elt.payload_type = rpk.x509.SignedManifest [static]

Reimplemented from `rpk.publication.publication_object_elt`.

Definition at line 309 of file publication.py.

The documentation for this class was generated from the following file:

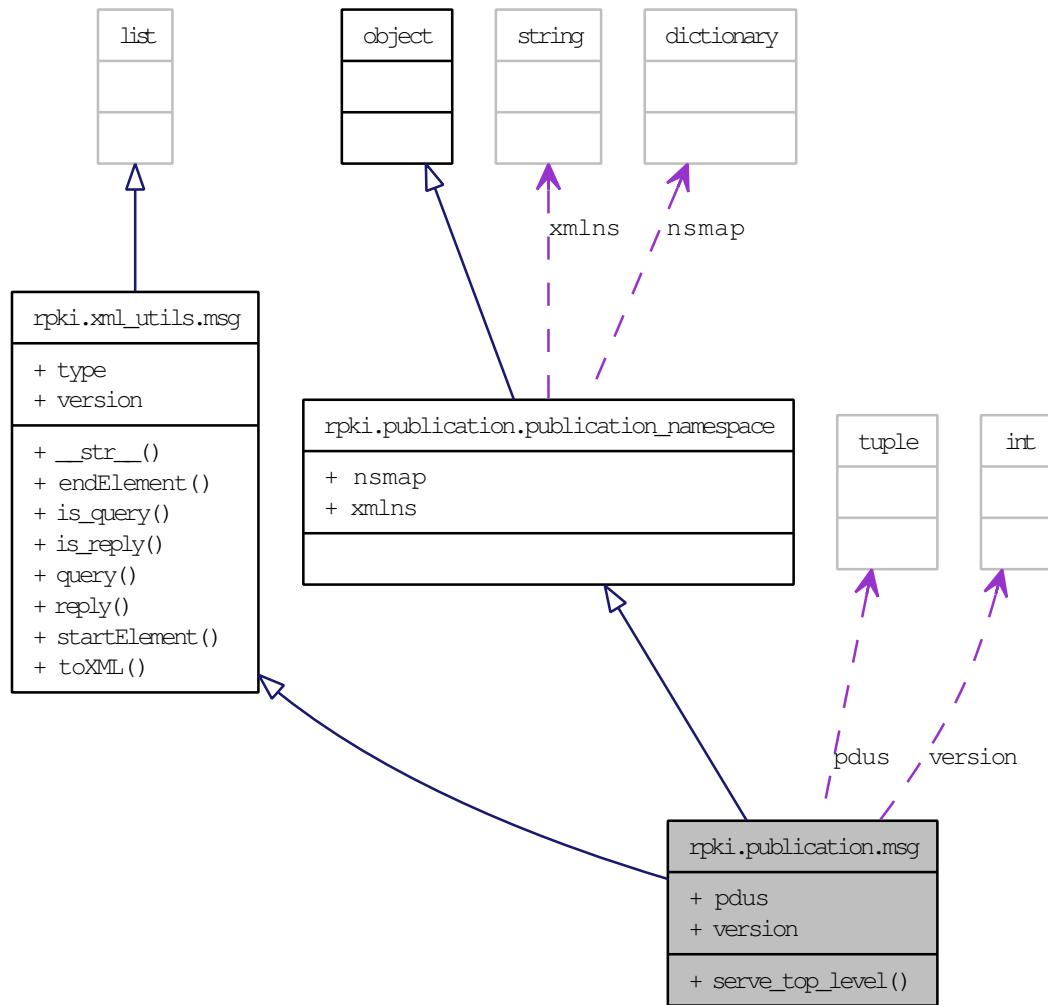
- `publication.py` (3107)

10.139 rpk.publication.msg Class Reference

Inherits `rpk::xml_utils::msg`, and `rpk::publication::publication_namespace`.

Inherited by `irbe_cli.publication_msg`.

Collaboration diagram for rpk.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.

10.139.1 Detailed Description

Publication PDU.

Definition at line 362 of file publication.py.

10.139.2 Member Function Documentation

10.139.2.1 def rpk.publication.msg.serve_top_level (*self*, *gctx*, *client*, *cb*)

Serve one msg PDU.

Definition at line 376 of file publication.py.

10.139.3 Member Data Documentation

10.139.3.1 rpk::publication.msg::pdus [static]

Initial value:

```
dict((x.element_name, x)
     for x in (config_elt, client_elt, certificate_elt, crl_elt, manifest_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.

10.139.3.2 rpk::publication.msg::version = 1 [static]

Protocol version.

Reimplemented from [rpk.xml_utils.msg](#).

Definition at line 369 of file publication.py.

The documentation for this class was generated from the following file:

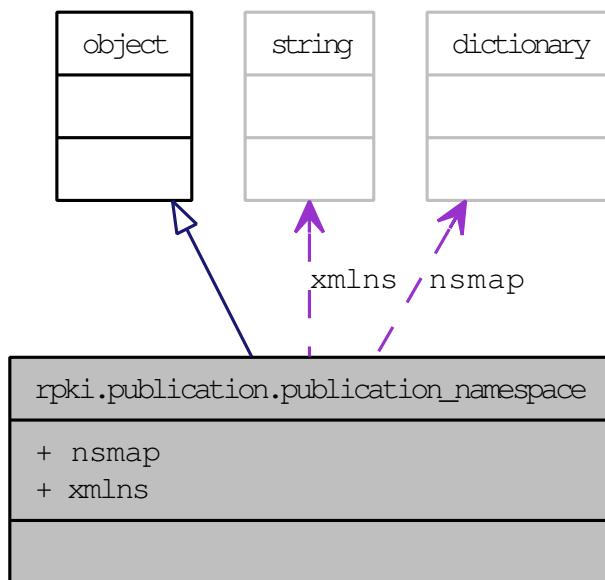
- publication.py (3107)

10.140 rpk.publication.publication_namespace Class Reference

Inherits [object](#).

Inherited by [rpk.publication.control_elt](#), [rpk.publication.msg](#), [rpk.publication.publication_object_elt](#), and [rpk.publication.report_error_elt](#).

Collaboration diagram for rpk.publication.publication_namespace:



Static Public Attributes

- dictionary `nsmap` = { None : `xmlns` }
- string `xmlns` = "http://www.hactrn.net/uris/rpki/publication-spec/"

10.140.1 Detailed Description

XML namespace parameters for publication protocol.

Definition at line 39 of file publication.py.

10.140.2 Member Data Documentation

10.140.2.1 `dictionary rpkি.publication.publication_namespace.nsmap = { None : xmlns } [static]`

Definition at line 45 of file publication.py.

10.140.2.2 `string rpkি.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:

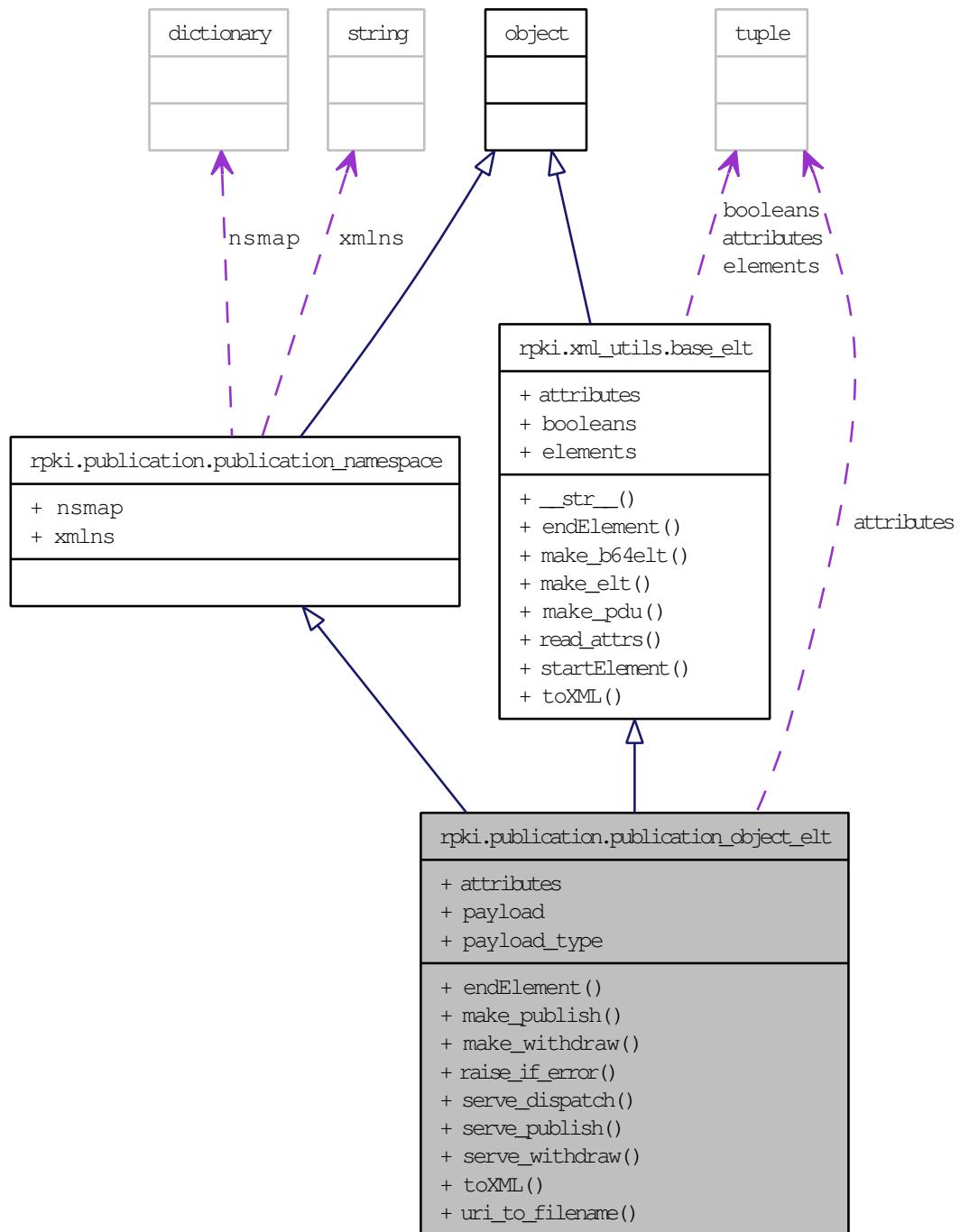
- [publication.py \(3107\)](#)

10.141 rpkি.publication.publication_object_elt Class Reference

Inherits [rpkি::xml_utils::base_elt](#), and [rpkি::publication::publication_namespace](#).

Inherited by [rpkি.publication.certificate_elt](#), [rpkি.publication.crl_elt](#), [rpkি.publication.manifest_elt](#), and [rpkি.publication.roa_elt](#).

Collaboration diagram for rpkি.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

10.141.1 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.

10.141.2 Member Function Documentation

10.141.2.1 def rpk.publication.publication_object_elt.endElement (*self, stack, name, text*)

Handle a publishable element element.

Reimplemented from [rpk.xml_utils.base_elt](#).

Definition at line 178 of file publication.py.

**10.141.2.2 def rpkি.publication.publication_object_elt.make_publish (*cls*, *uri*,
obj, *tag* = **None**)**

Construct a publication PDU.

Definition at line 266 of file publication.py.

**10.141.2.3 def rpkি.publication.publication_object_elt.make_withdraw (*cls*,
uri, *obj*, *tag* = **None**)**

Construct a withdrawal PDU.

Definition at line 274 of file publication.py.

10.141.2.4 def rpkি.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.

**10.141.2.5 def rpkি.publication.publication_object_elt.serve_dispatch (*self*,
r_msg, *cb*, *eb*)**

Action dispatch handler.

Definition at line 196 of file publication.py.

10.141.2.6 def rpkি.publication.publication_object_elt.serve_publish (*self*)

Publish an object.

Definition at line 221 of file publication.py.

10.141.2.7 def rpk.publication.publication_object_elt.serve_withdraw (self)

Withdraw an object.

Definition at line 236 of file publication.py.

10.141.2.8 def rpk.publication.publication_object_elt.toXML (self)

Generate XML element for publishable object.

Reimplemented from [rpk.xml_utils.base_elt](#).

Definition at line 187 of file publication.py.

10.141.2.9 def rpk.publication.publication_object_elt.uri_to_filename (self)

Convert a URI to a local filename.

Definition at line 250 of file publication.py.

10.141.3 Member Data Documentation**10.141.3.1 tuple rpk.publication.publication_object_elt.attributes = ("action", "tag", "client_handle", "uri") [static]**

XML attributes for this element.

Reimplemented from [rpk.xml_utils.base_elt](#).

Definition at line 174 of file publication.py.

10.141.3.2 rpk.publication.publication_object_elt.payload = None [static]

Definition at line 176 of file publication.py.

**10.141.3.3 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:

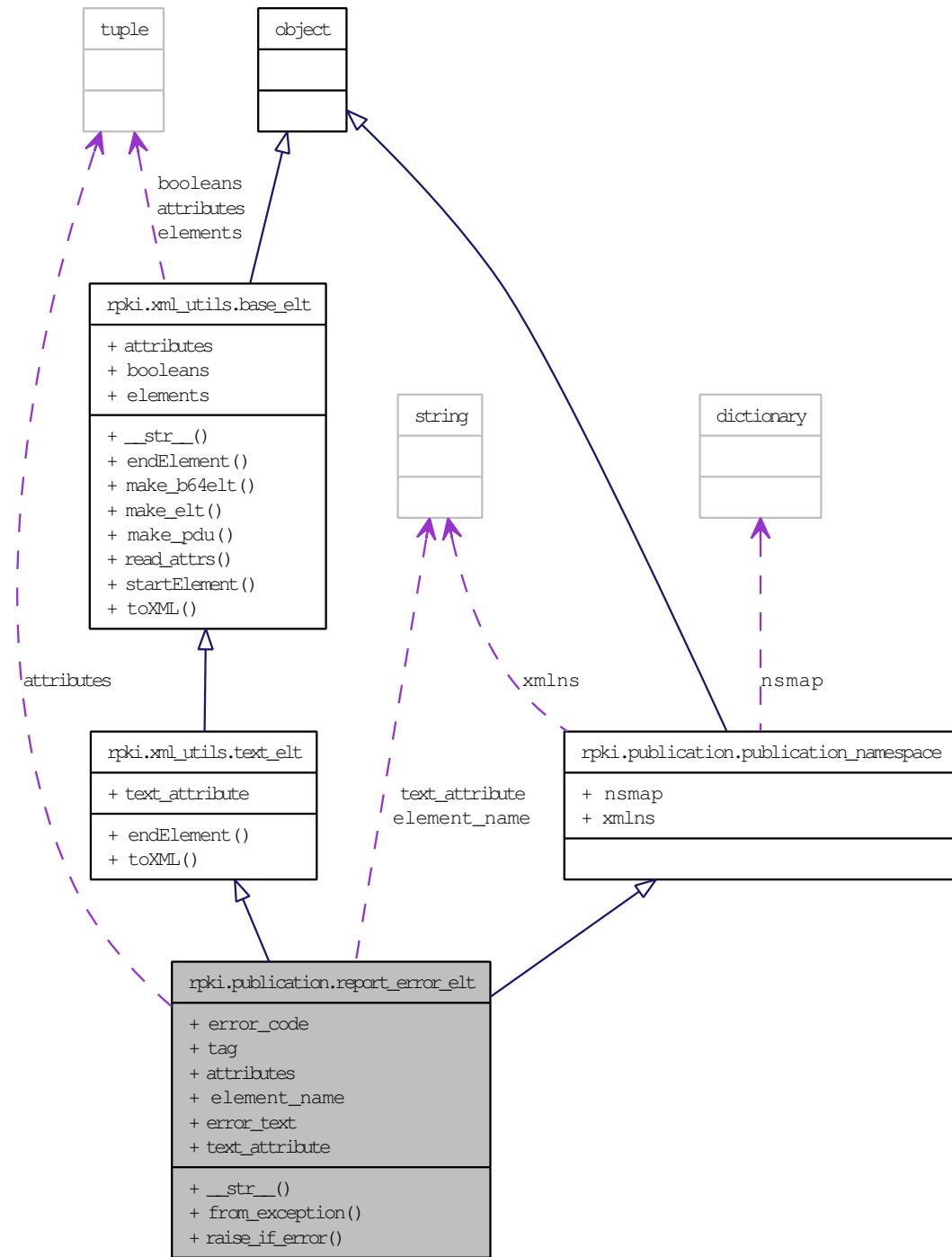
- [publication.py \(3107\)](#)

10.142 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 rpkি.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.

10.142.1 Detailed Description

<report_error/> element.

Definition at line 321 of file publication.py.

10.142.2 Member Function Documentation

10.142.2.1 def rpk.publication.report_error_elt.__str__ (*self*)

Convert a base_elt object to string format.

Reimplemented from [rpk.xml_utils.base_elt](#).

Definition at line 343 of file publication.py.

10.142.2.2 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.

10.142.2.3 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.

10.142.3 Member Data Documentation**10.142.3.1 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.

10.142.3.2 string rpki.publication.report_error_elt.element_name = "report_error" [static]

Definition at line 326 of file publication.py.

10.142.3.3 rpki.publication.report_error_elt.error_code

Definition at line 339 of file publication.py.

10.142.3.4 rpki.publication.report_error_elt.error_text = None [static]

Definition at line 330 of file publication.py.

10.142.3.5 rpki.publication.report_error_elt.tag

Definition at line 338 of file publication.py.

10.142.3.6 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:

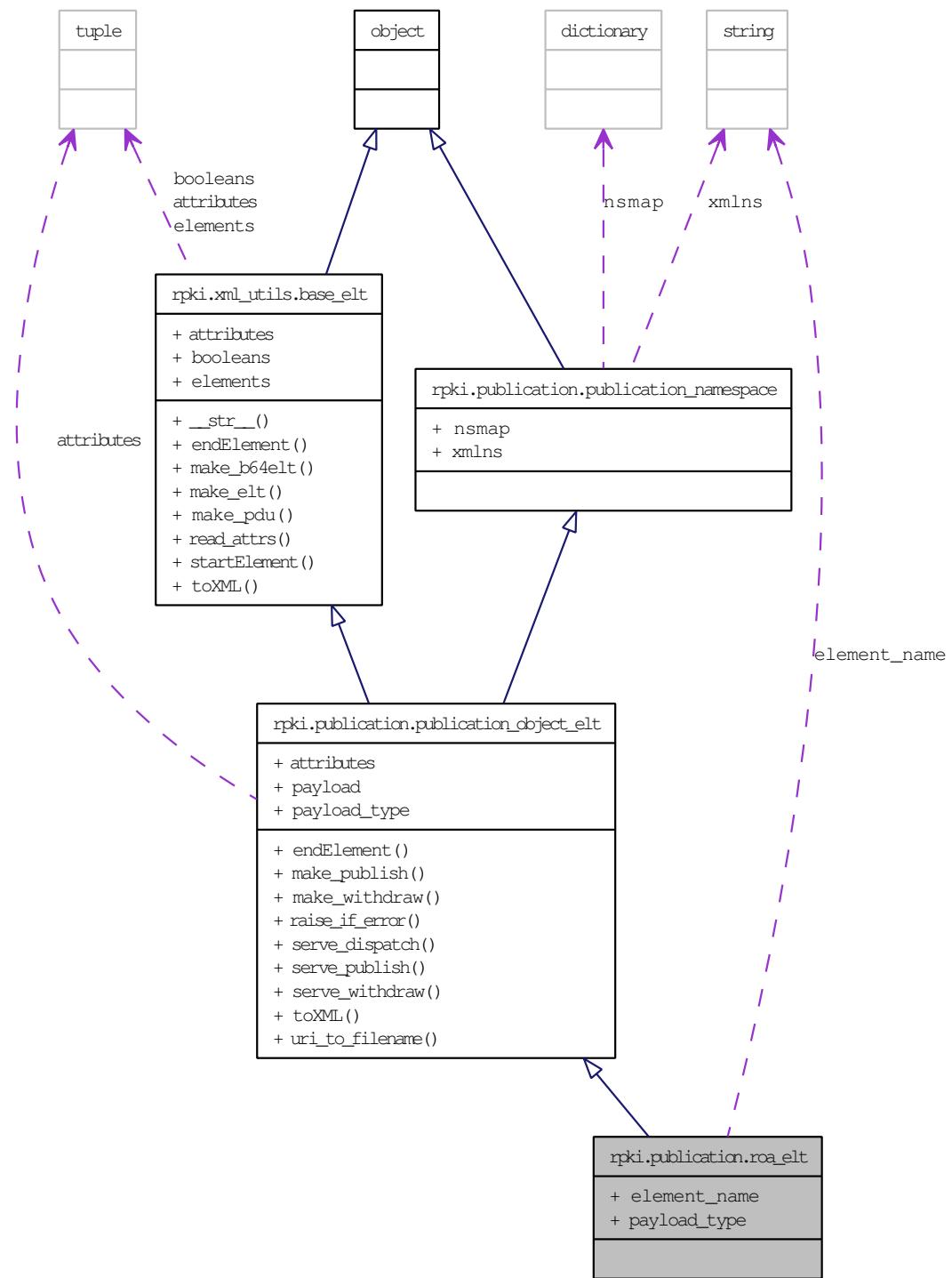
- [publication.py \(3107\)](#)

10.143 rpki.publication.roa_elt Class Reference

Inherits [rpki::publication::publication_object_elt](#).

Inherited by [irbe_cli.roa_elt](#).

Collaboration diagram for rpkি.publication.roa_elt:



Static Public Attributes

- string `element_name` = "roa"
- `payload_type` = `rpkি.x509.ROA`

10.143.1 Detailed Description

`<roa/>` element.

Definition at line 311 of file publication.py.

10.143.2 Member Data Documentation

10.143.2.1 string `rpkি.publication.roa_elt.element_name` = "roa" [static]

Definition at line 316 of file publication.py.

10.143.2.2 `rpkি.publication.roa_elt.payload_type` = `rpkি.x509.ROA` [static]

Reimplemented from `rpkি.publication.publication_object_elt`.

Definition at line 317 of file publication.py.

The documentation for this class was generated from the following file:

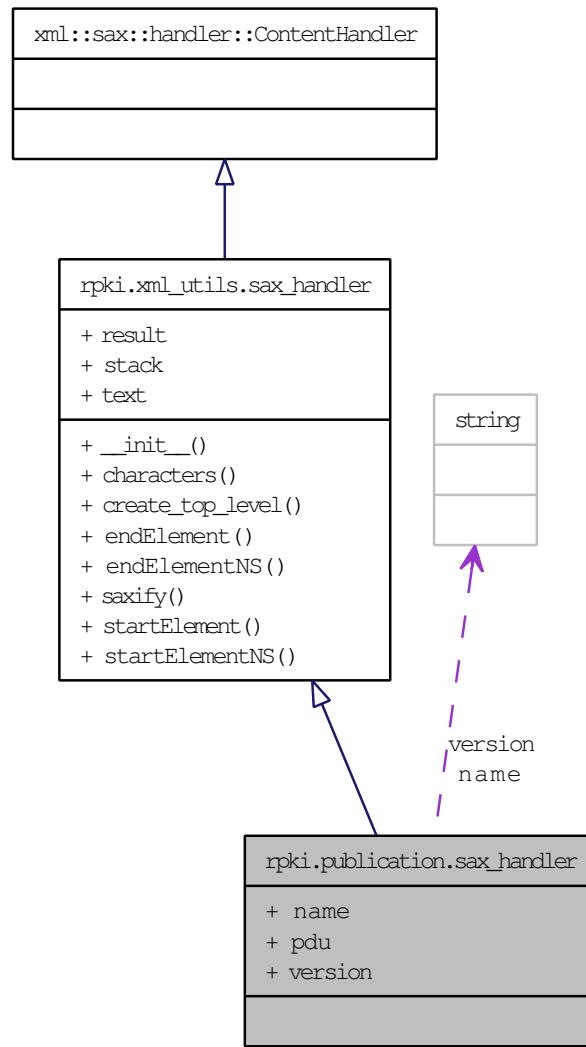
- `publication.py` (3107)

10.144 rpkি.publication.sax_handler Class Reference

Inherits `rpkি::xml_utils::sax_handler`.

Inherited by `irbe_cli.publication_sax_handler`.

Collaboration diagram for rpkি.publication.sax_handler:



Static Public Attributes

- string `name` = "msg"
- `pdu` = `msg`
- string `version` = "1"

10.144.1 Detailed Description

SAX handler for publication protocol.

Definition at line 406 of file publication.py.

10.144.2 Member Data Documentation

10.144.2.1 string rpkি.publication.sax_handler.name = "msg" [static]

Definition at line 412 of file publication.py.

10.144.2.2 rpkি.publication.sax_handler.pdu = msg [static]

Reimplemented in [irbe_cli.publication_sax_handler](#).

Definition at line 411 of file publication.py.

10.144.2.3 string rpkি.publication.sax_handler.version = "1" [static]

Definition at line 413 of file publication.py.

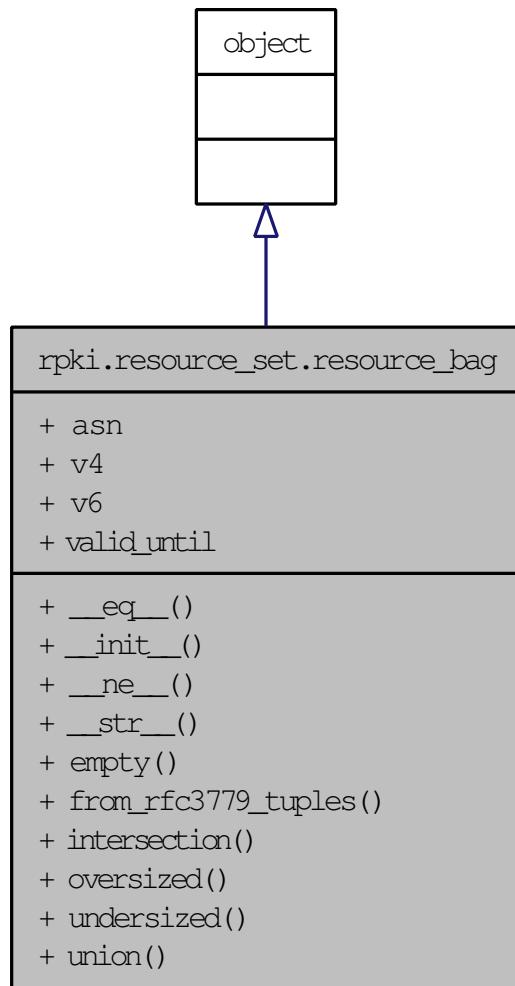
The documentation for this class was generated from the following file:

- [publication.py \(3107\)](#)

10.145 rpkি.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.

10.145.1 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.

10.145.2 Member Function Documentation

10.145.2.1 def rpkি.resource_set.resource_bag.__eq__(self, other)

Definition at line 615 of file resource_set.py.

10.145.2.2 def rpkি.resource_set.resource_bag.__init__(self, asn = None, v4 = None, v6 = None, valid_until = None)

Definition at line 565 of file resource_set.py.

10.145.2.3 def rpkি.resource_set.resource_bag.__ne__ (self, other)

Definition at line 621 of file resource_set.py.

10.145.2.4 def rpkি.resource_set.resource_bag.__str__ (self)

Definition at line 644 of file resource_set.py.

10.145.2.5 def rpkি.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.

10.145.2.6 def rpkি.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.

10.145.2.7 def rpkি.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.

10.145.2.8 def rpkি.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.

10.145.2.9 def rpkি.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.

10.145.2.10 def rpkি.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.

10.145.3 Member Data Documentation**10.145.3.1 rpkি::resource_set.resource_bag::asn**

Set of Autonomous System Number resources.

Definition at line 566 of file resource_set.py.

10.145.3.2 rpkি::resource_set.resource_bag::v4

Set of IPv4 resources.

Definition at line 567 of file resource_set.py.

10.145.3.3 rpkি::resource_set.resource_bag::v6

Set of IPv6 resources.

Definition at line 568 of file resource_set.py.

10.145.3.4 rpkি::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:

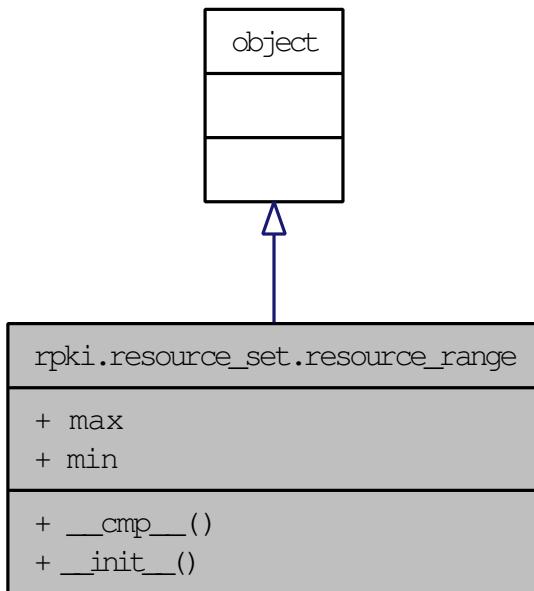
- [resource_set.py \(3107\)](#)

10.146 rpkি.resource_set.resource_range Class Reference

Inherits [object](#).

Inherited by [rpkি.resource_set.resource_range_as](#), and [rpkি.resource_set.resource_range_ip](#).

Collaboration diagram for rpkি.resource_set.resource_range:



Public Member Functions

- def [__cmp__](#)
- def [__init__](#)

Public Attributes

- [max](#)

- [min](#)

10.146.1 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`.

10.146.2 Member Function Documentation

10.146.2.1 def rpkি.resource_set.resource_range.__cmp__ (*self, other*)

Compare two `resource_range` objects.

Definition at line 67 of file `resource_set.py`.

10.146.2.2 def rpkি.resource_set.resource_range.__init__ (*self, min, max*)

Initialize and sanity check a `resource_range`.

Definition at line 59 of file `resource_set.py`.

10.146.3 Member Data Documentation

10.146.3.1 rpkি.resource_set.resource_range.max

Definition at line 65 of file `resource_set.py`.

10.146.3.2 rpkি.resource_set.resource_range.min

Reimplemented in [rpkি.resource_set.resource_range_as](#).

Definition at line 64 of file `resource_set.py`.

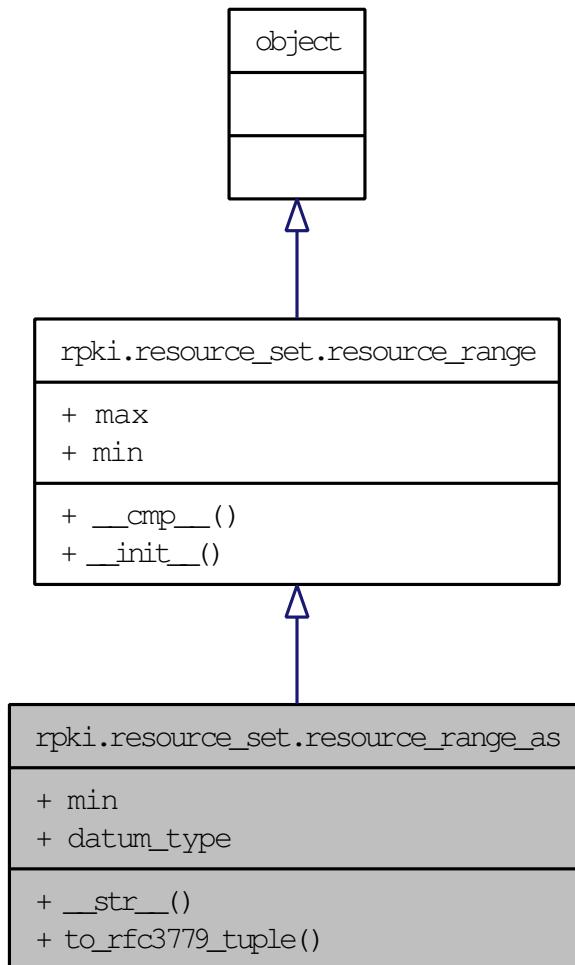
The documentation for this class was generated from the following file:

- [resource_set.py \(3107\)](#)

10.147 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).

10.147.1 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.

10.147.2 Member Function Documentation

10.147.2.1 def rpkি.resource_set.resource_range_as.__str__(self)

Convert a `resource_range_as` to string format.

Definition at line 91 of file resource_set.py.

10.147.2.2 def rpkি.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.

10.147.3 Member Data Documentation

10.147.3.1 rpkি::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.

10.147.3.2 rpkি.resource_set.resource_range_as.min

Reimplemented from [rpkি.resource_set.resource_range](#).

Definition at line 95 of file resource_set.py.

The documentation for this class was generated from the following file:

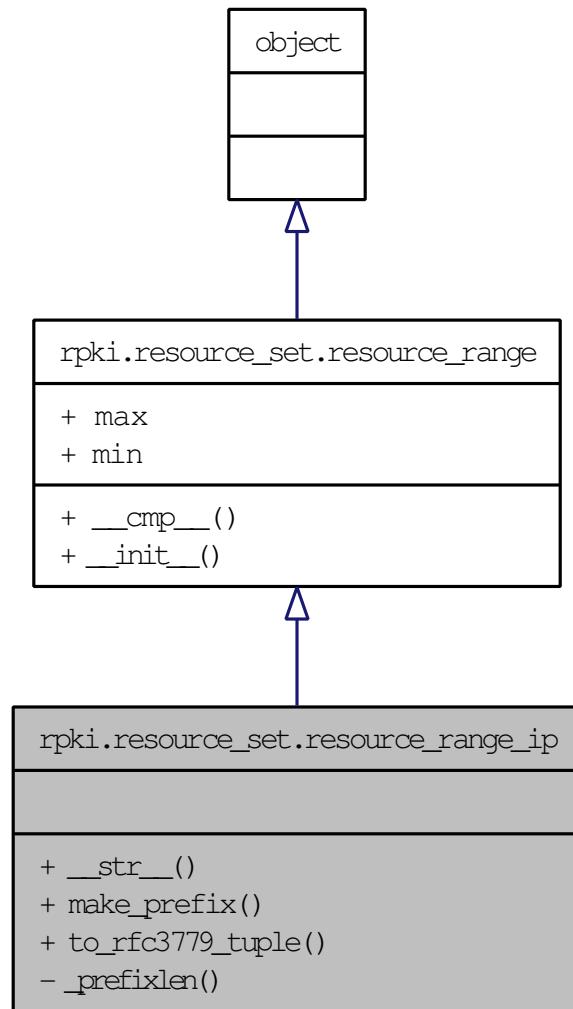
- [resource_set.py \(3107\)](#)

10.148 rpkি.resource_set.resource_range_ip Class Reference

Inherits [rpkি::resource_set::resource_range](#).

Inherited by [rpkি.resource_set.resource_range_ipv4](#), and [rpkি.resource_set.resource_range_ipv6](#).

Collaboration diagram for rpkি.resource_set.resource_range_ip:



Public Member Functions

- def `__str__`
- def `make_prefix`
- def `to_rfc3779_tuple`

Private Member Functions

- def [_prefixlen](#)

10.148.1 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.

10.148.2 Member Function Documentation

10.148.2.1 def rpkি.resource_set.resource_range_ip.__str__ (*self*)

Convert a resource_range_ip to string format.

Definition at line 137 of file resource_set.py.

10.148.2.2 def rpkি.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.

10.148.2.3 def rpkি.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.

10.148.2.4 def rpkি.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.

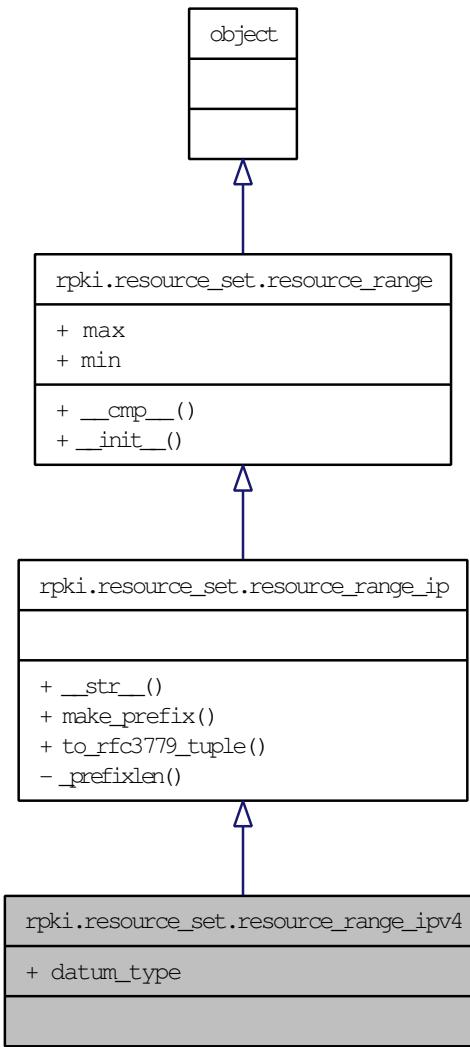
The documentation for this class was generated from the following file:

- [resource_set.py \(3107\)](#)

10.149 rpkি.resource_set.resource_range_ipv4 Class Reference

Inherits [rpkি::resource_set::resource_range_ip](#).

Collaboration diagram for rpkি.resource_set.resource_range_ipv4:



Static Public Attributes

- `datum_type = rpkি.ipaddrs.v4addr`
Type of underlying data (min and max).

10.149.1 Detailed Description

Range of IPv4 addresses.

Definition at line 170 of file resource_set.py.

10.149.2 Member Data Documentation

10.149.2.1 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.

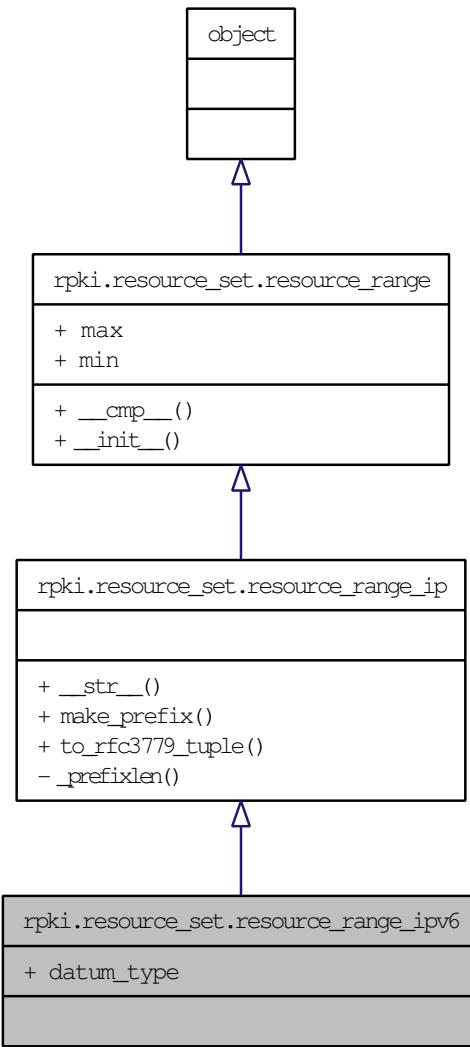
The documentation for this class was generated from the following file:

- [resource_set.py \(3107\)](#)

10.150 rpki.resource_set.resource_range_ipv6 Class Reference

Inherits [rpki::resource_set::resource_range_ip](#).

Collaboration diagram for rpkি.resource_set.resource_range_ipv6:



Static Public Attributes

- **datum_type** = [rpkি.ipaddrs.v6addr](#)
Type of underlying data (min and max).

10.150.1 Detailed Description

Range of IPv6 addresses.

Definition at line 180 of file resource_set.py.

10.150.2 Member Data Documentation

10.150.2.1 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:

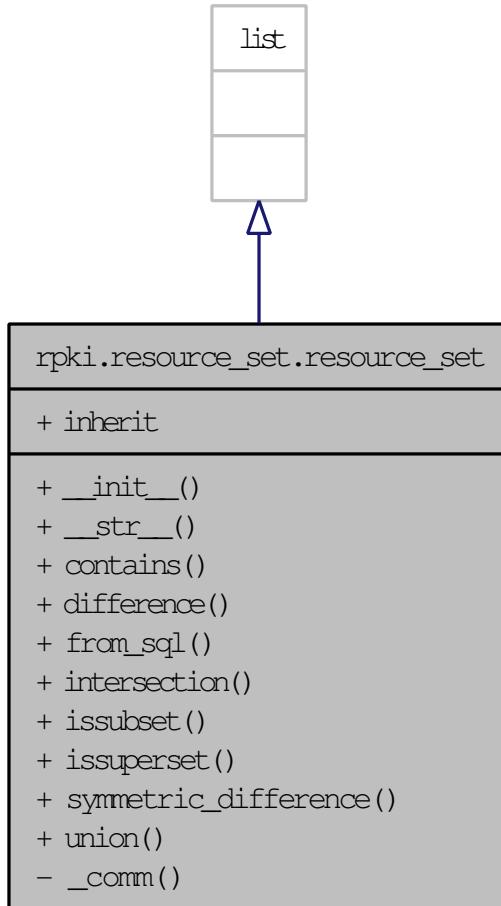
- [resource_set.py \(3107\)](#)

10.151 rpkি.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`

10.151.1 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`.

10.151.2 Member Function Documentation

10.151.2.1 def rpkি.resource_set.resource_set.__init__ (`self, ini = None`)

Initialize a `resource_set`.

Definition at line 219 of file `resource_set.py`.

10.151.2.2 def rpkি.resource_set.resource_set.__str__ (`self`)

Convert a `resource_set` to string format.

Definition at line 246 of file `resource_set.py`.

10.151.2.3 def rpkি.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.

10.151.2.4 def rpkি.resource_set.resource_set.contains (*self, item*)

Set membership test for resource sets.

Definition at line 332 of file resource_set.py.

10.151.2.5 def rpkি.resource_set.resource_set.difference (*self, other*)

Set difference for resource sets.

Definition at line 323 of file resource_set.py.

10.151.2.6 def rpkি.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.

10.151.2.7 def rpkি.resource_set.resource_set.intersection (*self, other*)

Set intersection for resource sets.

Definition at line 319 of file resource_set.py.

10.151.2.8 def rpkি.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.

10.151.2.9 def rpkি.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.

10.151.2.10 def rpkি.resource_set.resource_set.symmetric_difference (*self*, *other*)

Set symmetric difference (XOR) for resource sets.

Definition at line 327 of file resource_set.py.

10.151.2.11 def rpkি.resource_set.resource_set.union (*self*, *other*)

Set union for resource sets.

Definition at line 288 of file resource_set.py.

10.151.3 Member Data Documentation**10.151.3.1 rpkি::resource_set.resource_set::inherit = False [static]**

Boolean indicating whether this [resource_set](#) uses RFC 3779 inheritance.

Reimplemented in [rpkি.resource_set.resource_set_as](#), and [rpkি.resource_set.resource_set_ip](#).

Definition at line 217 of file resource_set.py.

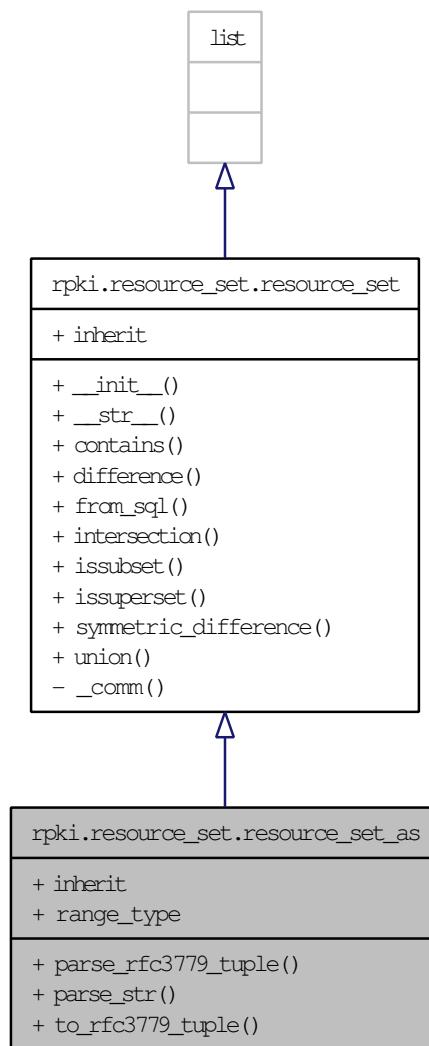
The documentation for this class was generated from the following file:

- [resource_set.py \(3107\)](#)

10.152 rpkি.resource_set.resource_set_as Class Reference

Inherits [rpkি.resource_set::resource_set](#).

Collaboration diagram for rpkি.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](#).

10.152.1 Detailed Description

Autonomous System Number resource set.

Definition at line 384 of file [resource_set.py](#).

10.152.2 Member Function Documentation

10.152.2.1 def rpkি.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](#).

10.152.2.2 def rpkি.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](#).

10.152.2.3 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.

10.152.3 Member Data Documentation**10.152.3.1 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.

**10.152.3.2 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:

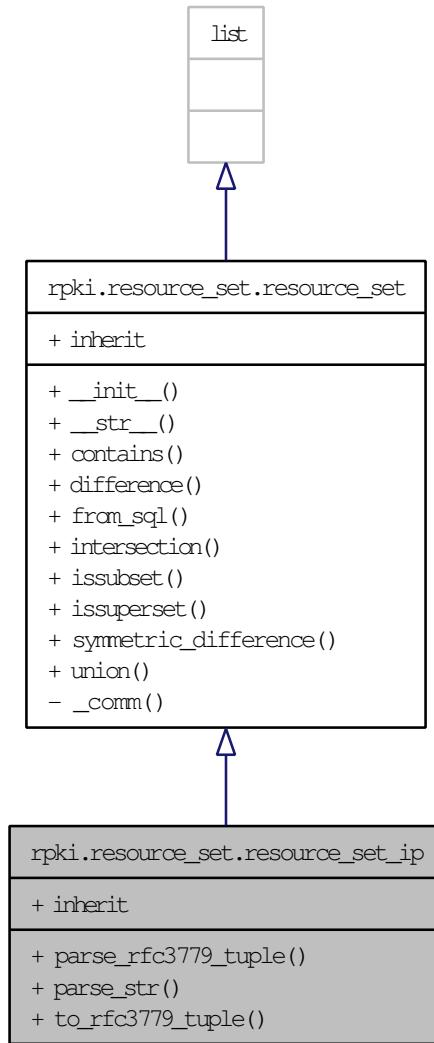
- [resource_set.py \(3107\)](#)

10.153 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.

10.153.1 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`.

10.153.2 Member Function Documentation

10.153.2.1 def rpkি.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`.

10.153.2.2 def rpkি.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`.

10.153.2.3 def rpkি.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`.

10.153.3 Member Data Documentation

10.153.3.1 rpkি.resource_set.resource_set_ip.inherit

Boolean indicating whether this [resource_set](#) uses RFC 3779 inheritance.

Reimplemented from [rpkি.resource_set.resource_set](#).

Definition at line 470 of file [resource_set.py](#).

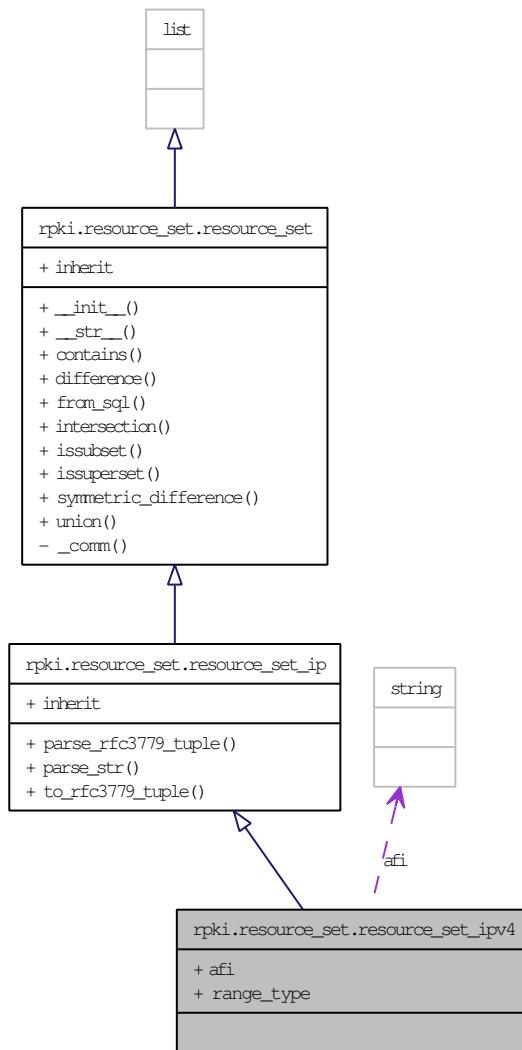
The documentation for this class was generated from the following file:

- [resource_set.py \(3107\)](#)

10.154 rpkি.resource_set.resource_set_ipv4 Class Reference

Inherits [rpkি::resource_set::resource_set_ip](#).

Collaboration diagram for rpkি.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`.

10.154.1 Detailed Description

IPv4 address resource set.

Definition at line 484 of file resource_set.py.

10.154.2 Member Data Documentation

10.154.2.1 rpkি::resource_set.resource_set_ipv4::afi = "\x00\x01" [static]

Address Family Identifier value for IPv4.

Definition at line 497 of file resource_set.py.

10.154.2.2 rpkি::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.

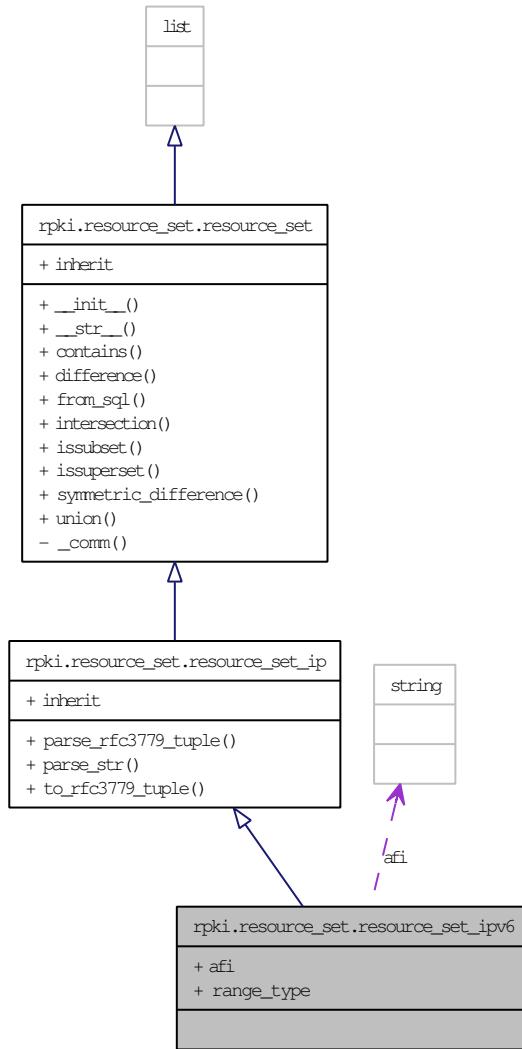
The documentation for this class was generated from the following file:

- [resource_set.py \(3107\)](#)

10.155 rpkি.resource_set.resource_set_ipv6 Class Reference

Inherits [rpkি::resource_set::resource_set_ip](#).

Collaboration diagram for rpkি.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`.

10.155.1 Detailed Description

IPv6 address resource set.

Definition at line 499 of file `resource_set.py`.

10.155.2 Member Data Documentation

10.155.2.1 `rpkি::resource_set.resource_set_ipv6::afi = "\x00\x02" [static]`

Address Family Identifier value for IPv6.

Definition at line 512 of file `resource_set.py`.

10.155.2.2 `rpkি::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:

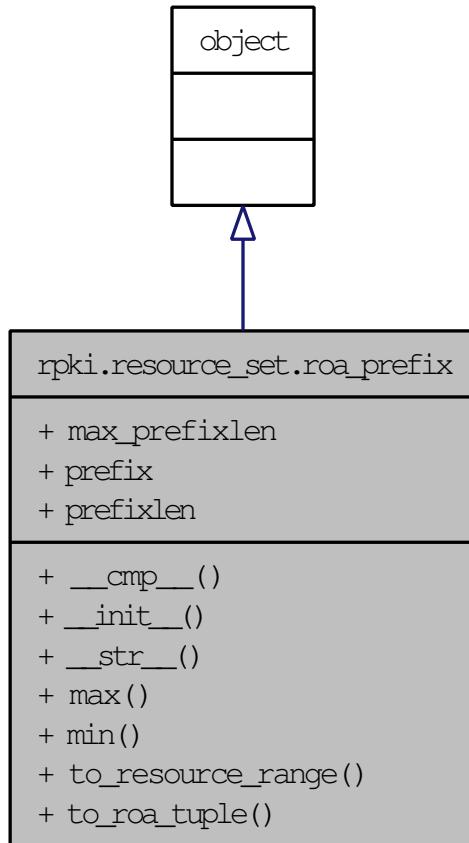
- [resource_set.py \(3107\)](#)

10.156 rpkি.resource_set.roa_prefix Class Reference

Inherits [object](#).

Inherited by [rpkি.resource_set.roa_prefix_ipv4](#), and [rpkি.resource_set.roa_prefix_ip6](#).

Collaboration diagram for rpkি.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.

10.156.1 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.

10.156.2 Member Function Documentation

10.156.2.1 def rpkি.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.

10.156.2.2 def rpkি.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.

10.156.2.3 def rpkি.resource_set.roa_prefix.__str__ (self)

Convert a ROA prefix to string format.

Definition at line 710 of file resource_set.py.

10.156.2.4 def rpkি.resource_set.roa_prefix.max (*self*)

Return highest address covered by prefix.

Definition at line 731 of file resource_set.py.

10.156.2.5 def rpkি.resource_set.roa_prefix.min (*self*)

Return lowest address covered by prefix.

Definition at line 727 of file resource_set.py.

10.156.2.6 def rpkি.resource_set.roa_prefix.to_resource_range (*self*)

Convert this ROA prefix to the equivalent resource_range_ip object. This is an irreversible transformation because it loses the max_prefixlen attribute, nothing we can do about that.

Definition at line 719 of file resource_set.py.

10.156.2.7 def rpkি.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.

10.156.3 Member Data Documentation**10.156.3.1 rpkি::resource_set.roa_prefix::max_prefixlen**

Maxmimum prefix length.

Definition at line 695 of file resource_set.py.

10.156.3.2 rpkি::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.

10.156.3.3 rpkি::resource_set.roa_prefix::prefixlen

(Minimum) prefix length.

Definition at line 694 of file resource_set.py.

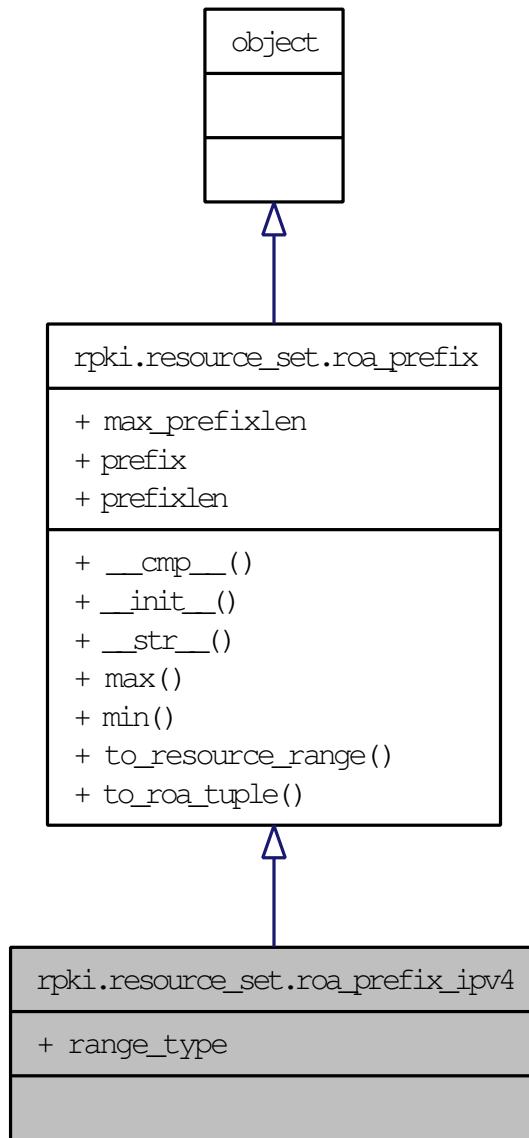
The documentation for this class was generated from the following file:

- [resource_set.py \(3107\)](#)

10.157 rpkি.resource_set.roa_prefix_ipv4 Class Reference

Inherits [rpkি::resource_set::roa_prefix](#).

Collaboration diagram for rpkি.resource_set.roa_prefix_ipv4:



Static Public Attributes

- `range_type = resource_range_ipv4`
Type of corresponding `resource_range_ip`.

10.157.1 Detailed Description

IPv4 ROA prefix.

Definition at line 746 of file resource_set.py.

10.157.2 Member Data Documentation

10.157.2.1 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.

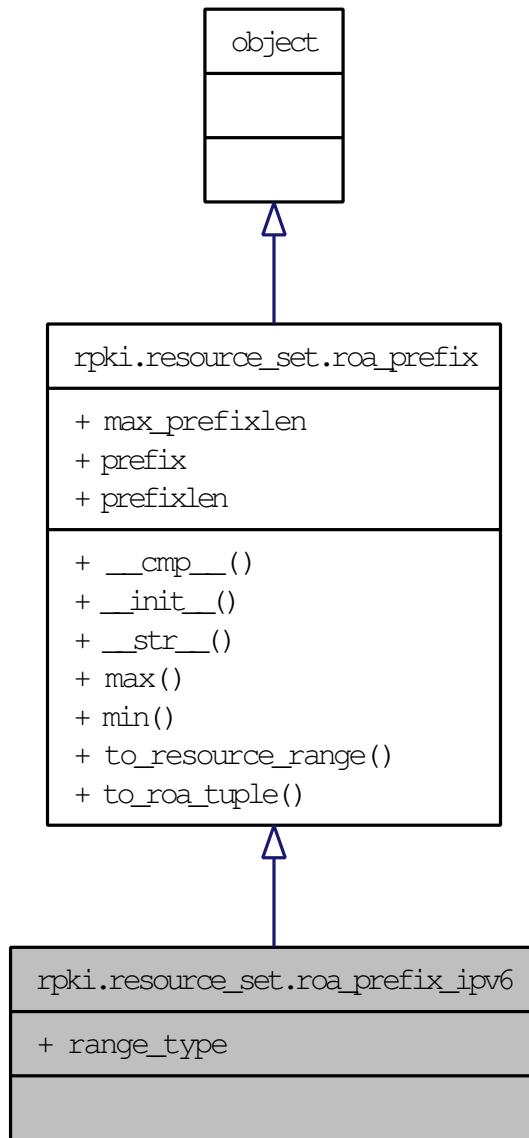
The documentation for this class was generated from the following file:

- [resource_set.py \(3107\)](#)

10.158 rpki.resource_set.roa_prefix_ipv6 Class Reference

Inherits [rpki::resource_set::roa_prefix](#).

Collaboration diagram for rpkি.resource_set.roa_prefix_ipv6:



Static Public Attributes

- `range_type = resource_range_ipv6`
Type of corresponding `resource_range_ip`.

10.158.1 Detailed Description

IPv6 ROA prefix.

Definition at line 756 of file resource_set.py.

10.158.2 Member Data Documentation

10.158.2.1 rpkি::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:

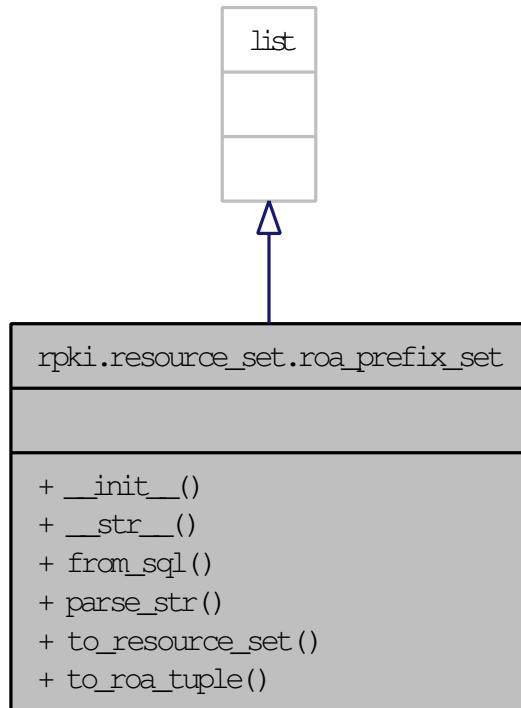
- [resource_set.py \(3107\)](#)

10.159 rpkি.resource_set.roa_prefix_set Class Reference

Inherits list.

Inherited by [rpkি.resource_set.roa_prefix_set_ipv4](#), and [rpkি.resource_set.roa_prefix_set_ipv6](#).

Collaboration diagram for rpkি.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](#)

10.159.1 Detailed Description

Set of ROA prefixes, analogous to the `resource_set_ip` class.

Definition at line 766 of file `resource_set.py`.

10.159.2 Member Function Documentation

10.159.2.1 def rpkি.resource_set.roa_prefix_set.__init__ (*self*, *ini* = **None**)

Initialize a ROA prefix set.

Definition at line 771 of file resource_set.py.

10.159.2.2 def rpkি.resource_set.roa_prefix_set.__str__ (*self*)

Convert a ROA prefix set to string format.

Definition at line 791 of file resource_set.py.

10.159.2.3 def rpkি.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.

10.159.2.4 def rpkি.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.

10.159.2.5 def rpkি.resource_set.roa_prefix_set.to_resource_set (*self*)

Convert a ROA prefix set to a resource set. This is an irreversible 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`.

10.159.2.6 def rpkি.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`.

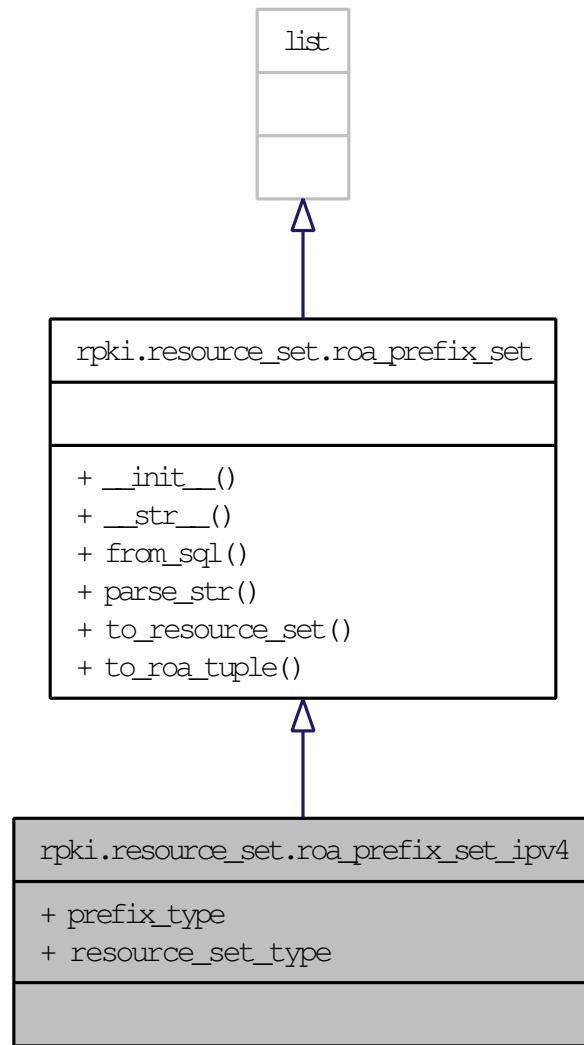
The documentation for this class was generated from the following file:

- [resource_set.py \(3107\)](#)

10.160 rpkি.resource_set.roa_prefix_set_ipv4 Class Reference

Inherits [rpkি::resource_set::roa_prefix_set](#).

Collaboration diagram for rpkি.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.

10.160.1 Detailed Description

Set of IPv4 ROA prefixes.

Definition at line 850 of file resource_set.py.

10.160.2 Member Data Documentation

10.160.2.1 rpkি::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.

10.160.2.2 rpkি::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.

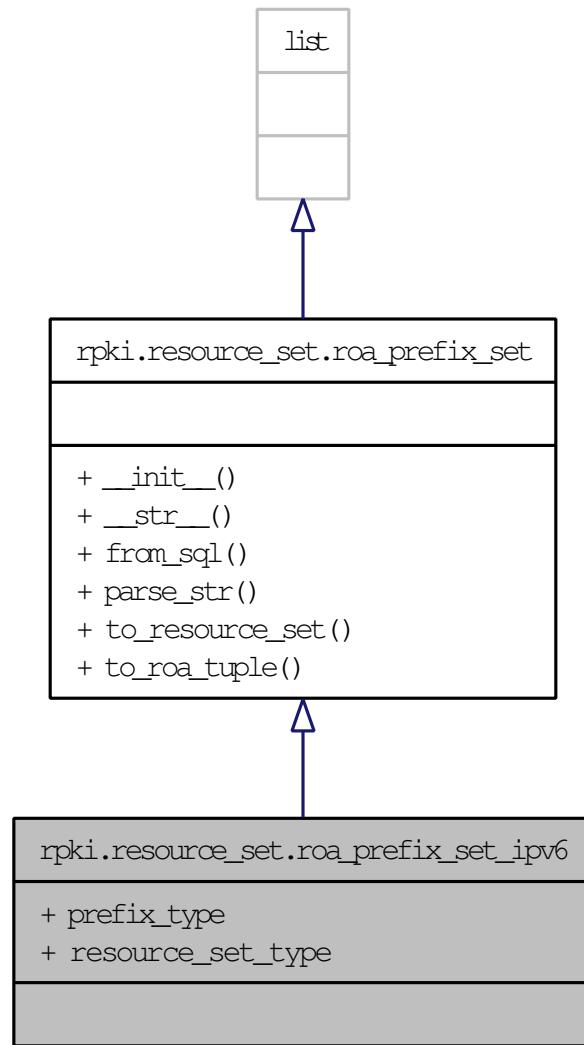
The documentation for this class was generated from the following file:

- [resource_set.py \(3107\)](#)

10.161 rpkি.resource_set.roa_prefix_set_ipv6 Class Reference

Inherits [rpkি::resource_set::roa_prefix_set](#).

Collaboration diagram for rpkি.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.

10.161.1 Detailed Description

Set of IPv6 ROA prefixes.

Definition at line 865 of file resource_set.py.

10.161.2 Member Data Documentation

10.161.2.1 `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.

10.161.2.2 `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.

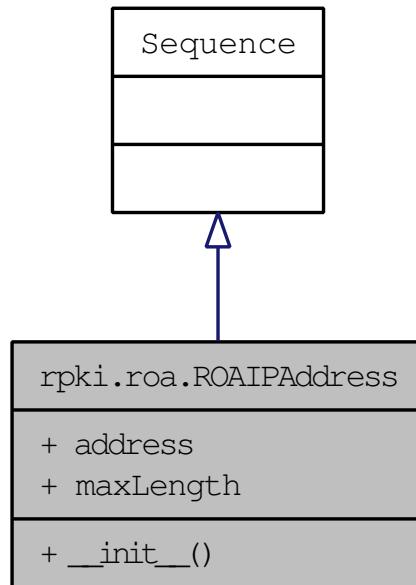
The documentation for this class was generated from the following file:

- [resource_set.py \(3107\)](#)

10.162 rpki.roa.ROAIPAddress Class Reference

Inherits [Sequence](#).

Collaboration diagram for rpki.roa.ROAIPAddress:



Public Member Functions

- def [__init__](#)

Public Attributes

- [address](#)
- [maxLength](#)

10.162.1 Detailed Description

Definition at line 47 of file roa.py.

10.162.2 Member Function Documentation

10.162.2.1 def rpki.roa.ROAIPAddress.__init__(self, optional=0, default="")

Definition at line 48 of file roa.py.

10.162.3 Member Data Documentation

10.162.3.1 rpki.roa.ROAIPAddress.address

Definition at line 49 of file roa.py.

10.162.3.2 rpki.roa.ROAIPAddress.maxLength

Definition at line 50 of file roa.py.

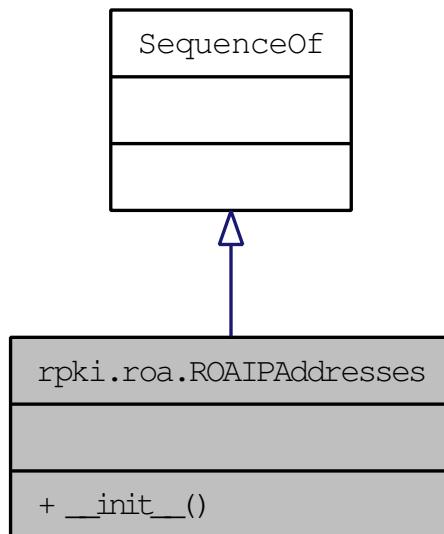
The documentation for this class was generated from the following file:

- [roa.py \(2424\)](#)

10.163 rpki.roa.ROAIPAddresses Class Reference

Inherits [SequenceOf](#).

Collaboration diagram for rpki.roa.ROAIPAddresses:



Public Member Functions

- def [__init__](#)

10.163.1 Detailed Description

Definition at line 54 of file roa.py.

10.163.2 Member Function Documentation

10.163.2.1 def rpkি.roa.ROAIPAddresses.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 55 of file roa.py.

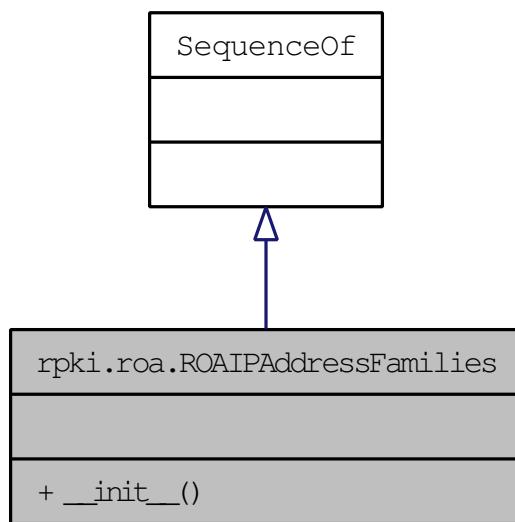
The documentation for this class was generated from the following file:

- [roa.py \(2424\)](#)

10.164 rpkি.roa.ROAIPAddressFamilies Class Reference

Inherits [SequenceOf](#).

Collaboration diagram for rpkি.roa.ROAIPAddressFamilies:



Public Member Functions

- def [__init__](#)

10.164.1 Detailed Description

Definition at line 65 of file roa.py.

10.164.2 Member Function Documentation

10.164.2.1 def rpkি.roa.ROAIPAddressFamilies.__init__ (*self*, *optional* = 0, *default* = "")

Definition at line 66 of file roa.py.

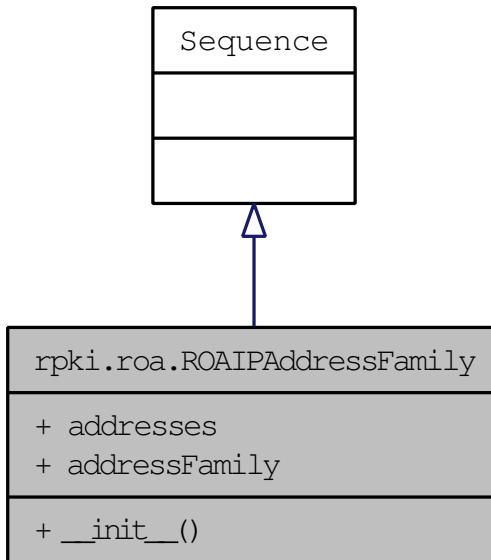
The documentation for this class was generated from the following file:

- [roa.py \(2424\)](#)

10.165 rpkি.roa.ROAIPAddressFamily Class Reference

Inherits [Sequence](#).

Collaboration diagram for rpki.roa.ROAIPAddressFamily:



Public Member Functions

- def [__init__](#)

Public Attributes

- [addresses](#)
- [addressFamily](#)

10.165.1 Detailed Description

Definition at line 58 of file roa.py.

10.165.2 Member Function Documentation

10.165.2.1 def rpki.roa.ROAIPAddressFamily.__init__ (*self*, *optional* = 0, *default* = "")

Definition at line 59 of file roa.py.

10.165.3 Member Data Documentation

10.165.3.1 rpki.roa.ROAIPAddressFamily.addresses

Definition at line 61 of file roa.py.

10.165.3.2 rpki.roa.ROAIPAddressFamily.addressFamily

Definition at line 60 of file roa.py.

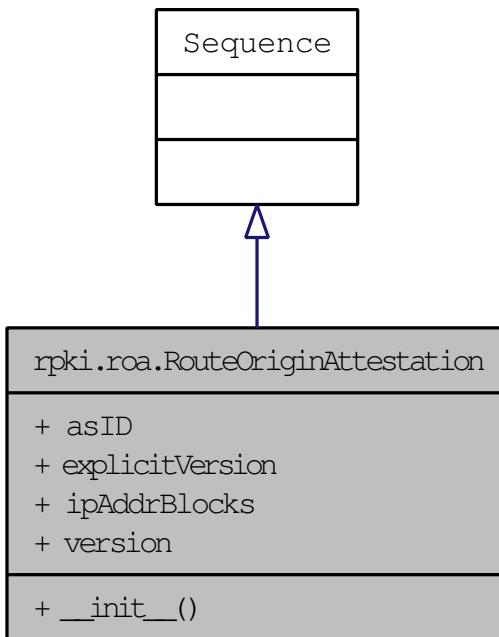
The documentation for this class was generated from the following file:

- [roa.py \(2424\)](#)

10.166 rpki.roa.RouteOriginAttestation Class Reference

Inherits [Sequence](#).

Collaboration diagram for rpki.roa.RouteOriginAttestation:



Public Member Functions

- def [__init__](#)

Public Attributes

- [asID](#)
- [explicitVersion](#)
- [ipAddrBlocks](#)
- [version](#)

10.166.1 Detailed Description

Definition at line 69 of file roa.py.

10.166.2 Member Function Documentation

10.166.2.1 def rpkি.roa.RouteOriginAttestation.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 70 of file roa.py.

10.166.3 Member Data Documentation

10.166.3.1 rpkি.roa.RouteOriginAttestation.asID

Definition at line 73 of file roa.py.

10.166.3.2 rpkি.roa.RouteOriginAttestation.explicitVersion

Definition at line 72 of file roa.py.

10.166.3.3 rpkি.roa.RouteOriginAttestation.ipAddrBlocks

Definition at line 74 of file roa.py.

10.166.3.4 rpki.roa.RouteOriginAttestation.version

Definition at line 71 of file roa.py.

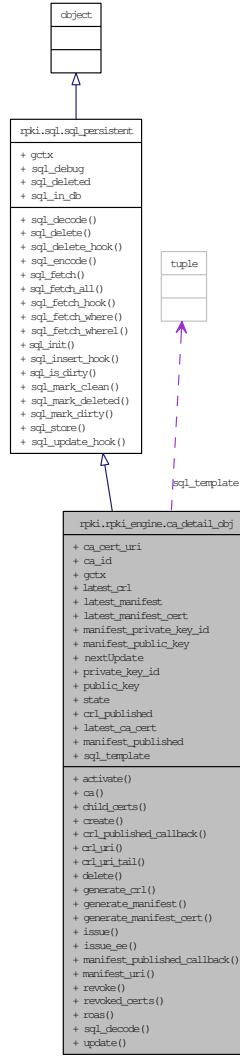
The documentation for this class was generated from the following file:

- [roa.py \(2424\)](#)

10.167 rpki.rpki_engine.ca_detail_obj Class Reference

Inherits [rpki::sql::sql_persistent](#).

Collaboration diagram for rpkি.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`

10.167.1 Detailed Description

Internal CA detail object.

Definition at line 562 of file rpkirpki_engine.py.

10.167.2 Member Function Documentation

10.167.2.1 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.

10.167.2.2 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.

10.167.2.3 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.

10.167.2.4 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.

10.167.2.5 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.

10.167.2.6 def rpkirpki_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.

10.167.2.7 def rpkirpki_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.

**10.167.2.8 def rpkirpki_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.

**10.167.2.9 def rpkirpki_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.

**10.167.2.10 def rpkirpki_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.

10.167.2.11 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.

10.167.2.12 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.

10.167.2.13 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.

10.167.2.14 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.

10.167.2.15 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.

10.167.2.16 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.

10.167.2.17 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.

10.167.2.18 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.

10.167.2.19 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.

10.167.2.20 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.

10.167.3 Member Data Documentation**10.167.3.1 rpki.rpki_engine.ca_detail_obj.ca_cert_uri**

Definition at line 632 of file rpki_engine.py.

10.167.3.2 rpki.rpki_engine.ca_detail_obj.ca_id

Definition at line 768 of file rpki_engine.py.

10.167.3.3 rpki.rpki_engine.ca_detail_obj.crl_published = None [static]

Definition at line 584 of file rpki_engine.py.

10.167.3.4 rpki.rpki_engine.ca_detail_obj.gctx

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 767 of file rpki_engine.py.

10.167.3.5 rpki.rpki_engine.ca_detail_obj.latest_ca_cert = None [static]

Definition at line 586 of file rpki_engine.py.

10.167.3.6 rpki.rpki_engine.ca_detail_obj.latest_crl

Definition at line 872 of file rpki_engine.py.

10.167.3.7 rpki.rpki_engine.ca_detail_obj.latest_manifest

Definition at line 913 of file rpki_engine.py.

10.167.3.8 rpki.rpki_engine.ca_detail_obj.latest_manifest_cert

Definition at line 730 of file rpki_engine.py.

10.167.3.9 rpki.rpki_engine.ca_detail_obj.manifest_private_key_id

Definition at line 728 of file rpki_engine.py.

10.167.3.10 rpki.rpki_engine.ca_detail_obj.manifest_public_key

Definition at line 729 of file rpki_engine.py.

**10.167.3.11 rpki.rpki_engine.ca_detail_obj.manifest_published = None
[static]**

Definition at line 585 of file rpki_engine.py.

10.167.3.12 rpki.rpki_engine.ca_detail_obj.nextUpdate

Definition at line 706 of file rpki_engine.py.

10.167.3.13 rpki.rpki_engine.ca_detail_obj.private_key_id

Definition at line 727 of file rpki_engine.py.

10.167.3.14 rpki.rpki_engine.ca_detail_obj.public_key

Definition at line 772 of file rpki_engine.py.

10.167.3.15 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.

10.167.3.16 rpki.rpki_engine.ca_detail_obj.state

Definition at line 634 of file rpki_engine.py.

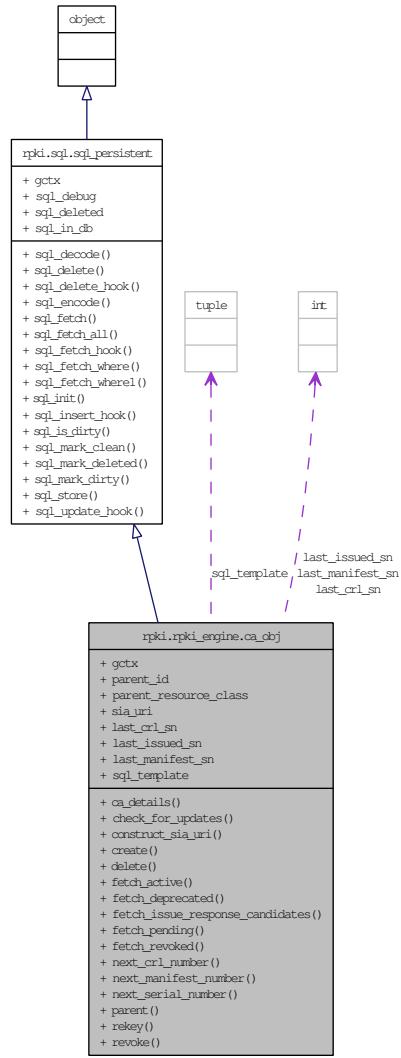
The documentation for this class was generated from the following file:

- [rpki_engine.py \(3107\)](#)

10.168 rpki.rpki_engine.ca_obj Class Reference

Inherits [rpki::sql::sql_persistent](#).

Collaboration diagram for rpkি.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`

10.168.1 Detailed Description

Internal CA object.

Definition at line 308 of file rpki_engine.py.

10.168.2 Member Function Documentation

10.168.2.1 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.

10.168.2.2 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.

10.168.2.3 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.

10.168.2.4 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.

10.168.2.5 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.

10.168.2.6 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.

10.168.2.7 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.

10.168.2.8 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.

10.168.2.9 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.

10.168.2.10 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.

10.168.2.11 def rpki.rpki_engine.ca_obj.next_crl_number (*self*)

Allocate a CRL serial number.

Definition at line 517 of file rpki_engine.py.

10.168.2.12 def rpki.rpki_engine.ca_obj.next_manifest_number (*self*)

Allocate a manifest serial number.

Definition at line 509 of file rpki_engine.py.

10.168.2.13 def rpki.rpki_engine.ca_obj.next_serial_number (*self*)

Allocate a certificate serial number.

Definition at line 501 of file rpki_engine.py.

10.168.2.14 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.

10.168.2.15 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.

10.168.2.16 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.

10.168.3 Member Data Documentation**10.168.3.1 rpki.rpki_engine.ca_obj.gctx**

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 458 of file rpki_engine.py.

10.168.3.2 int rpki.rpki_engine.ca_obj.last_crl_sn = 0 [static]

Definition at line 322 of file rpki_engine.py.

10.168.3.3 int rpki.rpki_engine.ca_obj.last_issued_sn = 0 [static]

Definition at line 323 of file rpki_engine.py.

10.168.3.4 int rpki.rpki_engine.ca_obj.last_manifest_sn = 0 [static]

Definition at line 324 of file rpki_engine.py.

10.168.3.5 rpki.rpki_engine.ca_obj.parent_id

Definition at line 459 of file rpki_engine.py.

10.168.3.6 rpki.rpki_engine.ca_obj.parent_resource_class

Definition at line 460 of file rpki_engine.py.

10.168.3.7 rpki.rpki_engine.ca_obj.sia_uri

Definition at line 382 of file rpki_engine.py.

10.168.3.8 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.

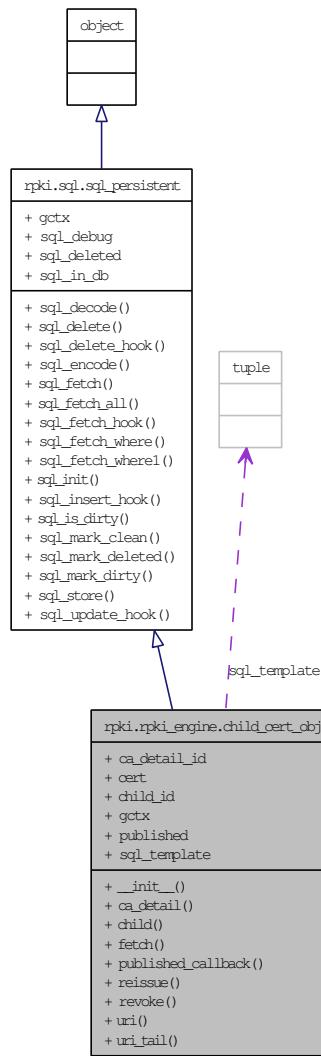
The documentation for this class was generated from the following file:

- [rpki_engine.py \(3107\)](#)

10.169 rpki.rpki_engine.child_cert_obj Class Reference

Inherits [rpki::sql::sql_persistent](#).

Collaboration diagram for rpkি.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](#)

10.169.1 Detailed Description

Certificate that has been issued to a child.

Definition at line 936 of file rpki_engine.py.

10.169.2 Member Function Documentation

10.169.2.1 def rpkirpki_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.

10.169.2.2 def rpkirpki_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.

10.169.2.3 def rpkirpki_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.

10.169.2.4 def rpkirpki_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.

10.169.2.5 def rpkirpki_engine.child_cert_obj.published_callback (self, pdu)

Publication callback: check result and mark published.

Definition at line 1080 of file rpki_engine.py.

10.169.2.6 def rpkirpki_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.

10.169.2.7 def rpkirpki_engine.child_cert_obj.revoke (self, publisher)

Revoke a child cert.

Definition at line 979 of file rpki_engine.py.

10.169.2.8 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.

10.169.2.9 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.

10.169.3 Member Data Documentation**10.169.3.1 rpki.rpki_engine.child_cert_obj.ca_detail_id**

Definition at line 957 of file rpki_engine.py.

10.169.3.2 rpki.rpki_engine.child_cert_obj.cert

Definition at line 958 of file rpki_engine.py.

10.169.3.3 rpki.rpki_engine.child_cert_obj.child_id

Definition at line 956 of file rpki_engine.py.

10.169.3.4 rpki.rpki_engine.child_cert_obj.gctx

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 955 of file rpki_engine.py.

10.169.3.5 rpki.rpki_engine.child_cert_obj.published

Definition at line 959 of file rpki_engine.py.

10.169.3.6 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.

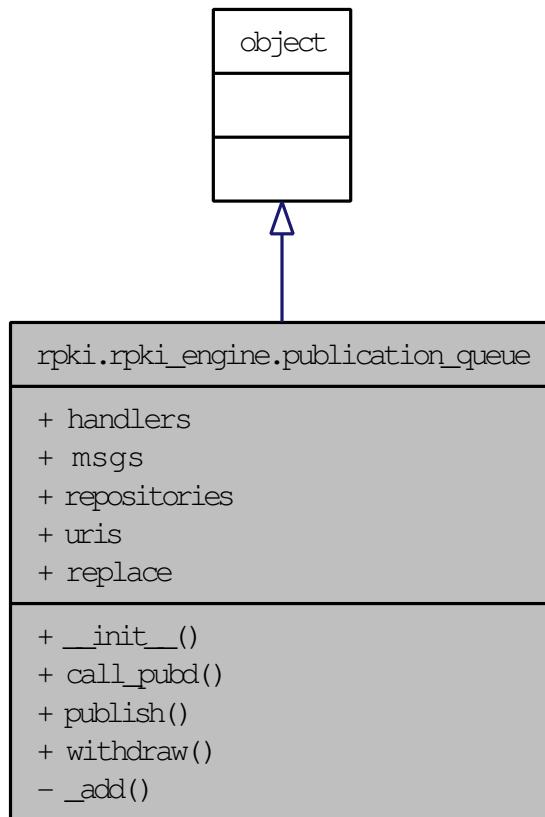
The documentation for this class was generated from the following file:

- [rpki_engine.py \(3107\)](#)

10.170 rpki.rpki_engine.publication_queue Class Reference

Inherits [object](#).

Collaboration diagram for rpkি.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`

10.170.1 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.

10.170.2 Member Function Documentation

10.170.2.1 def rpki.rpki_engine.publication_queue.__init__ (*self*)

Definition at line 1379 of file rpki_engine.py.

10.170.2.2 def rpki.rpki_engine.publication_queue._add (*self, cls, uri, obj, repository, handler, withdraw*) [private]

Definition at line 1386 of file rpki_engine.py.

10.170.2.3 def rpki.rpki_engine.publication_queue.call_pubd (*self, cb, eb*)

Definition at line 1409 of file rpki_engine.py.

10.170.2.4 def rpki.rpki_engine.publication_queue.publish (*self, cls, uri, obj, repository, handler = None*)

Definition at line 1403 of file rpki_engine.py.

10.170.2.5 def rpki.rpki_engine.publication_queue.withdraw (self, cls, uri, obj, repository, handler = None)

Definition at line 1406 of file rpki_engine.py.

10.170.3 Member Data Documentation

10.170.3.1 rpki.rpki_engine.publication_queue.handlers

Definition at line 1382 of file rpki_engine.py.

10.170.3.2 rpki.rpki_engine.publication_queue.msgs

Definition at line 1381 of file rpki_engine.py.

10.170.3.3 rpki.rpki_engine.publication_queue.replace = True [static]

Definition at line 1377 of file rpki_engine.py.

10.170.3.4 rpki.rpki_engine.publication_queue.repositories

Definition at line 1380 of file rpki_engine.py.

10.170.3.5 rpki.rpki_engine.publication_queue.uris

Definition at line 1384 of file rpki_engine.py.

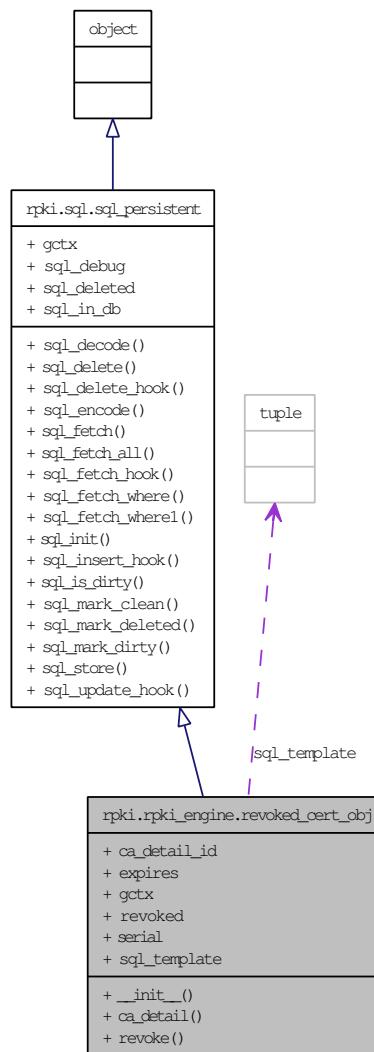
The documentation for this class was generated from the following file:

- [rpki_engine.py \(3107\)](#)

10.171 rpkি.rpki_engine.revoked_cert_obj Class Reference

Inherits [rpkি::sql::sql_persistent](#).

Collaboration diagram for rpkি.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](#)

10.171.1 Detailed Description

Tombstone for a revoked certificate.

Definition at line 1088 of file rpki_engine.py.

10.171.2 Member Function Documentation

10.171.2.1 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.

10.171.2.2 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.

10.171.2.3 def rpki.rpki_engine.revoked_cert_obj.revoke (*cls, cert, ca_detail*)

Revoke a certificate.

Definition at line 1117 of file rpki_engine.py.

10.171.3 Member Data Documentation**10.171.3.1 rpki.rpki_engine.revoked_cert_obj.ca_detail_id**

Definition at line 1108 of file rpki_engine.py.

10.171.3.2 rpki.rpki_engine.revoked_cert_obj.expires

Definition at line 1107 of file rpki_engine.py.

10.171.3.3 rpki.rpki_engine.revoked_cert_obj.gctx

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 1104 of file rpki_engine.py.

10.171.3.4 rpki.rpki_engine.revoked_cert_obj.revoked

Definition at line 1106 of file rpki_engine.py.

10.171.3.5 rpki.rpki_engine.revoked_cert_obj.serial

Definition at line 1105 of file rpki_engine.py.

10.171.3.6 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.

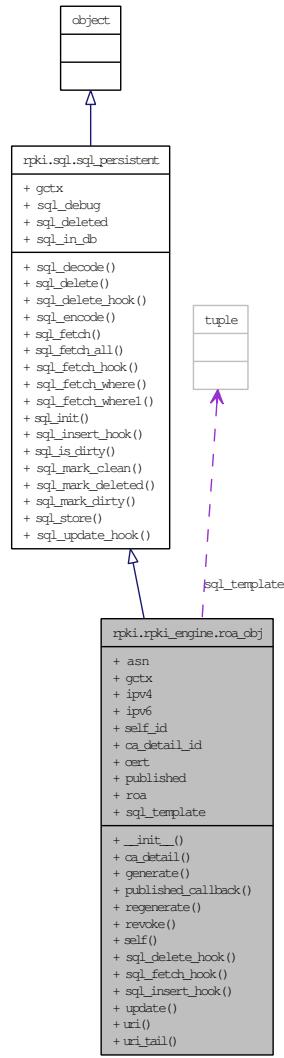
The documentation for this class was generated from the following file:

- [rpki_engine.py \(3107\)](#)

10.172 rpki.rpki_engine.roa_obj Class Reference

Inherits [rpki::sql::sql_persistent](#).

Collaboration diagram for rpkি.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](#)

10.172.1 Detailed Description

Route Origin Authorization.

Definition at line 1128 of file rpki_engine.py.

10.172.2 Member Function Documentation

10.172.2.1 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.

10.172.2.2 def rpkি.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.

10.172.2.3 def rpkি.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.

10.172.2.4 def rpkি.rpki_engine.roa_obj.published_callback (*self, pdu*)

Check publication result.

Definition at line 1303 of file rpki_engine.py.

10.172.2.5 def rpkি.rpki_engine.roa_obj.regenerate (*self, publisher*)

Reissue ROA associated with this roa_obj.

Definition at line 1343 of file rpki_engine.py.

10.172.2.6 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.

10.172.2.7 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.

10.172.2.8 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.

10.172.2.9 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.

10.172.2.10 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.

10.172.2.11 def rpki.rpki_engine.roa_obj.update (*self, publisher*)

Bring this roa_obj's ROA up to date if necessary.

Definition at line 1207 of file rpki_engine.py.

10.172.2.12 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.

10.172.2.13 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.

10.172.3 Member Data Documentation

10.172.3.1 rpki.rpki_engine.roa_obj.asn

Definition at line 1198 of file rpki_engine.py.

10.172.3.2 rpki.rpki_engine.roa_obj.ca_detail_id = None [static]

Definition at line 1143 of file rpki_engine.py.

10.172.3.3 rpki.rpki_engine.roa_obj.cert = None [static]

Definition at line 1144 of file rpki_engine.py.

10.172.3.4 rpki.rpki_engine.roa_obj.gctx

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 1196 of file rpki_engine.py.

10.172.3.5 rpki.rpki_engine.roa_obj.ipv4

Definition at line 1199 of file rpki_engine.py.

10.172.3.6 rpki.rpki_engine.roa_obj.ipv6

Definition at line 1200 of file rpki_engine.py.

10.172.3.7 rpki.rpki_engine.roa_obj.published = None [static]

Definition at line 1146 of file rpki_engine.py.

10.172.3.8 rpki.rpki_engine.roa_obj.roa = None [static]

Definition at line 1145 of file rpki_engine.py.

10.172.3.9 rpki.rpki_engine.roa_obj.self_id

Definition at line 1197 of file rpki_engine.py.

10.172.3.10 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 \(3107\)](#)

10.173 rpki.rpki_engine.rpkid_context Class Reference

Inherits [object](#).

Collaboration diagram for 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_regex = re.compile("/up-down/([-A-Z0-9_]+)/([-A-Z0-9_-]+)\$", re.I)

10.173.1 Detailed Description

A container for various global rpkid parameters.

Definition at line 39 of file rpkid_engine.py.

10.173.2 Member Function Documentation

10.173.2.1 def rpkid_context.__init__ (*self*, *cfg*)

Definition at line 44 of file rpkid_context.py.

10.173.2.2 def rpkid_context.build_https_ta_cache (*self*)

Build dynamic TLS trust anchors.

Definition at line 288 of file rpkid_context.py.

10.173.2.3 def rpkid_context.checkpoint (*self*)

Record that we were still alive when we got here, by resetting keepalive timer.

Definition at line 200 of file rpkid_context.py.

10.173.2.4 def rpkid_context.clear_https_ta_cache (*self*)

Clear dynamic TLS trust anchors.

Definition at line 279 of file rpkid_context.py.

10.173.2.5 def rpkid_context.cron (*self*, *cb* = **None**)

Periodic tasks.

Definition at line 207 of file rpkid_context.py.

10.173.2.6 def 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 rpkid_context.py.

10.173.2.7 def rpkid_context.irdb_query (self, q_pdu, callback, errback)

Perform an IRDB callback query.

Definition at line 86 of file rpkid_context.py.

10.173.2.8 def 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 rpkid_context.py.

10.173.2.9 def rpkid_context.irdb_query_roa_requests (self, self_handle, callback, errback)

Ask IRDB about self's ROA requests.

Definition at line 134 of file rpkid_context.py.

10.173.2.10 def rpkid_context.left_right_handler (self, query, path, cb)

Process one left-right PDU.

Definition at line 146 of file rpkid_context.py.

10.173.2.11 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.

**10.173.2.12 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.

10.173.3 Member Data Documentation**10.173.3.1 rpki.rpki_engine.rpkid_context.bpk1_ta**

Definition at line 48 of file rpki_engine.py.

10.173.3.2 rpki.rpki_engine.rpkid_context.cron_keepalive

Definition at line 68 of file rpki_engine.py.

10.173.3.3 rpki.rpki_engine.rpkid_context.cron_period

Definition at line 67 of file rpki_engine.py.

10.173.3.4 rpki.rpki_engine.rpkid_context.cron_timeout

Definition at line 71 of file rpki_engine.py.

10.173.3.5 rpki.rpki_engine.rpkid_context.cron_timer

Definition at line 79 of file rpki_engine.py.

10.173.3.6 rpki.rpki_engine.rpkid_context.https_server_host

Definition at line 56 of file rpki_engine.py.

10.173.3.7 rpki.rpki_engine.rpkid_context.https_server_port

Definition at line 57 of file rpki_engine.py.

**10.173.3.8 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.

10.173.3.9 rpki.rpki_engine.rpkid_context.initial_delay

Definition at line 63 of file rpki_engine.py.

10.173.3.10 rpki.rpki_engine.rpkid_context.irbe_cert

Definition at line 50 of file rpki_engine.py.

10.173.3.11 rpki.rpki_engine.rpkid_context.irdb_cert

Definition at line 49 of file rpki_engine.py.

10.173.3.12 rpki.rpki_engine.rpkid_context.irdb_url

Definition at line 54 of file rpki_engine.py.

10.173.3.13 rpki.rpki_engine.rpkid_context.publication_kludge_base

Definition at line 59 of file rpki_engine.py.

10.173.3.14 rpki.rpki_engine.rpkid_context.rpkid_cert

Definition at line 51 of file rpki_engine.py.

10.173.3.15 rpki.rpki_engine.rpkid_context.rpkid_key

Definition at line 52 of file rpki_engine.py.

10.173.3.16 rpki.rpki_engine.rpkid_context.sql

Definition at line 46 of file rpki_engine.py.

**10.173.3.17 tuple rpki.rpki_engine.rpkid_context.up_down_url_regex =
re.compile("/up-down/([-A-Z0-9_]+)/([-A-Z0-9_]+)\$", re.I)
[static]**

Definition at line 170 of file rpki_engine.py.

10.173.3.18 rpki.rpki_engine.rpkid_context.use_internal_cron

Definition at line 61 of file rpki_engine.py.

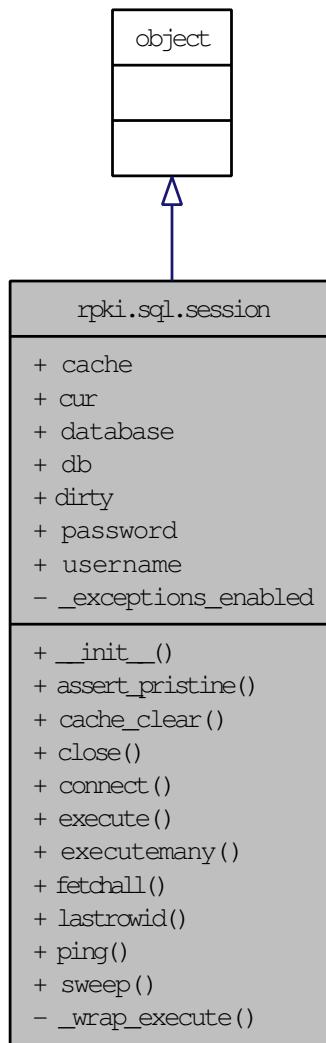
The documentation for this class was generated from the following file:

- [rpkি_engine.py \(3107\)](#)

10.174 rpkি.sql.session Class Reference

Inherits [object](#).

Collaboration diagram for rpkি.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

10.174.1 Detailed Description

SQL session layer.

Definition at line 50 of file sql.py.

10.174.2 Member Function Documentation

10.174.2.1 def rpkি.sql.session.__init__ (*self*, *cfg*)

Definition at line 57 of file sql.py.

10.174.2.2 def rpkি.sql.session._wrap_execute (*self*, *func*, *query*, *args*) [private]

Definition at line 88 of file sql.py.

10.174.2.3 def rpkি.sql.session.assert_pristine (*self*)

Assert that there are no dirty objects in the cache.

Definition at line 112 of file sql.py.

10.174.2.4 def rpkি.sql.session.cache_clear (*self*)

Clear the object cache.

Definition at line 108 of file sql.py.

10.174.2.5 def rpkি.sql.session.close (*self*)

Definition at line 77 of file sql.py.

10.174.2.6 def rpkি.sql.session.connect (*self*)

Definition at line 72 of file sql.py.

10.174.2.7 def rpki.sql.session.execute (*self*, *query*, *args* = **None)**

Definition at line 96 of file sql.py.

10.174.2.8 def rpki.sql.session.executemany (*self*, *query*, *args*)

Definition at line 99 of file sql.py.

10.174.2.9 def rpki.sql.session.fetchall (*self*)

Definition at line 102 of file sql.py.

10.174.2.10 def rpki.sql.session.lastrowid (*self*)

Definition at line 105 of file sql.py.

10.174.2.11 def rpki.sql.session.ping (*self*)

Definition at line 85 of file sql.py.

10.174.2.12 def rpki.sql.session.sweep (*self*)

Write any dirty objects out to SQL.

Definition at line 116 of file sql.py.

10.174.3 Member Data Documentation**10.174.3.1 rpki.sql.session._exceptions_enabled = False [static, private]**

Definition at line 55 of file sql.py.

10.174.3.2 rpki.sql.session.cache

Definition at line 67 of file sql.py.

10.174.3.3 rpki.sql.session.cur

Definition at line 74 of file sql.py.

10.174.3.4 rpki.sql.session.database

Definition at line 64 of file sql.py.

10.174.3.5 rpki.sql.session.db

Definition at line 73 of file sql.py.

10.174.3.6 rpki.sql.session.dirty

Definition at line 68 of file sql.py.

10.174.3.7 rpki.sql.session.password

Definition at line 65 of file sql.py.

10.174.3.8 rpki.sql.session.username

Definition at line 63 of file sql.py.

The documentation for this class was generated from the following file:

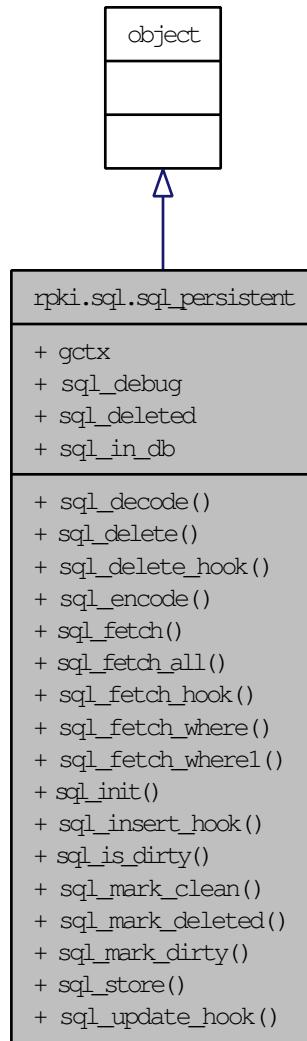
- [sql.py \(2895\)](#)

10.175 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 rpkি.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.

10.175.1 Detailed Description

Mixin for persistent class that needs to be stored in SQL.

Definition at line 152 of file [sql.py](#).

10.175.2 Member Function Documentation

10.175.2.1 def rpkysql.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 [rpkি.rpki_engine.ca_detail_obj](#).

Definition at line 322 of file sql.py.

10.175.2.2 def rpkি.sql.sql_persistent.sql_delete (*self*)

Delete this object from SQL.

Definition at line 293 of file sql.py.

10.175.2.3 def rpkি.sql.sql_persistent.sql_delete_hook (*self*)

Customization hook.

Reimplemented in [rpkি.rpki_engine.roa_obj](#).

Definition at line 348 of file sql.py.

10.175.2.4 def rpkি.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.

10.175.2.5 def rpkি.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.

10.175.2.6 def rpkি.sql.sql_persistent.sql_fetch_all (*cls, gctx*)

Fetch all objects of this type from SQL.

Definition at line 211 of file sql.py.

10.175.2.7 def rpkি.sql.sql_persistent.sql_fetch_hook (*self*)

Customization hook.

Reimplemented in [rpkি.rpki_engine.roa_obj](#).

Definition at line 335 of file sql.py.

10.175.2.8 def rpkি.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.

10.175.2.9 def rpkি.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.

10.175.2.10 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.

10.175.2.11 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.

10.175.2.12 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.

10.175.2.13 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.

10.175.2.14 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.

10.175.2.15 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.

10.175.2.16 def rpki.sql.sql_persistent.sql_store (*self*)

Store this object to SQL.

Definition at line 271 of file sql.py.

10.175.2.17 def rpki.sql.sql_persistent.sql_update_hook (*self*)

Customization hook.

Definition at line 343 of file sql.py.

10.175.3 Member Data Documentation**10.175.3.1 rpki.sql.sql_persistent.getx**

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.

10.175.3.2 rpki::sql.sql_persistent::sql_debug = False [static]

Enable logging of SQL actions.

Definition at line 170 of file sql.py.

10.175.3.3 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.

10.175.3.4 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.

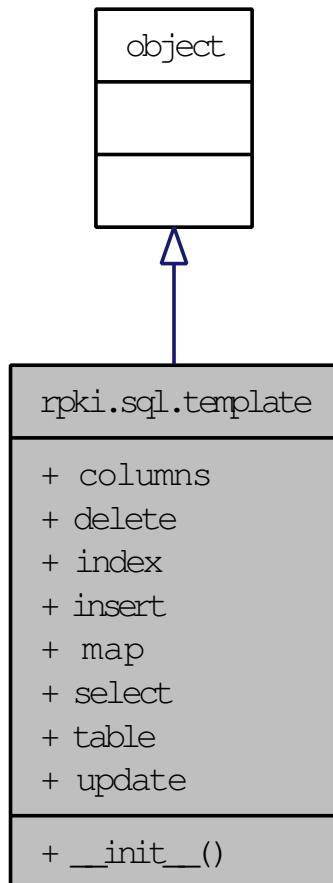
The documentation for this class was generated from the following file:

- [sql.py \(2895\)](#)

10.176 rpki.sql.template Class Reference

Inherits [object](#).

Collaboration diagram for rpkysql.template:



Public Member Functions

- def [__init__](#)

Public Attributes

- `columns`
- `delete`
- `index`
- `insert`
- `map`

- [select](#)
- [table](#)
- [update](#)

10.176.1 Detailed Description

SQL template generator.

Definition at line 128 of file sql.py.

10.176.2 Member Function Documentation

10.176.2.1 def rpkি.sql.template.__init__ (*self*, *table_name*, *index_column*, *data_columns*)

Build a SQL template.

Definition at line 133 of file sql.py.

10.176.3 Member Data Documentation

10.176.3.1 rpkি.sql.template.columns

Definition at line 140 of file sql.py.

10.176.3.2 rpkি.sql.template.delete

Definition at line 150 of file sql.py.

10.176.3.3 rpkি.sql.template.index

Definition at line 139 of file sql.py.

10.176.3.4 rpki.sql.template.insert

Definition at line 143 of file sql.py.

10.176.3.5 rpki.sql.template.map

Definition at line 141 of file sql.py.

10.176.3.6 rpki.sql.template.select

Definition at line 142 of file sql.py.

10.176.3.7 rpki.sql.template.table

Definition at line 138 of file sql.py.

10.176.3.8 rpki.sql.template.update

Definition at line 146 of file sql.py.

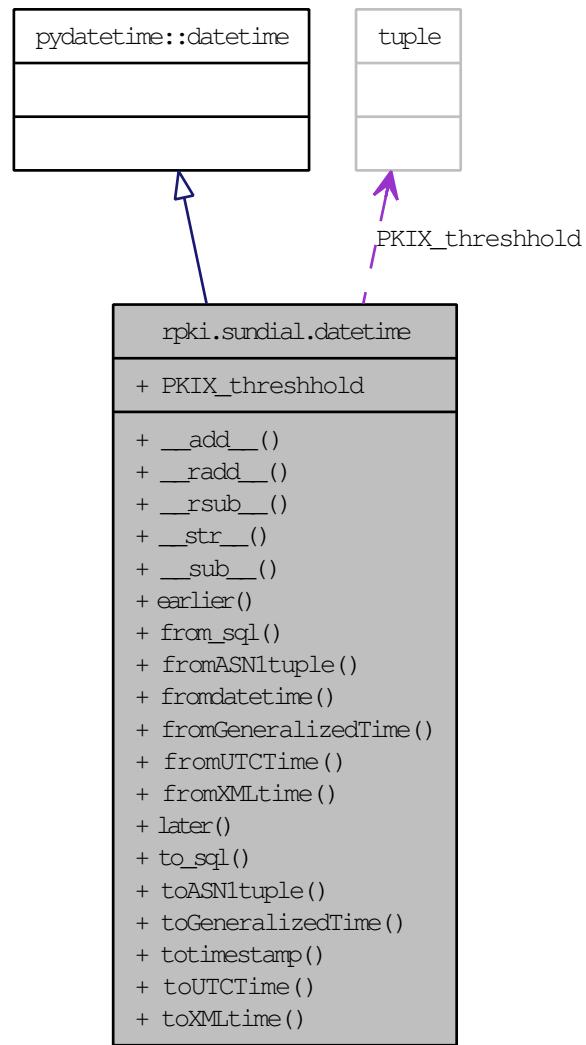
The documentation for this class was generated from the following file:

- [sql.py \(2895\)](#)

10.177 rpki.sundial.datetime Class Reference

Inherits [pydatetime::datetime](#).

Collaboration diagram for rpkisundial.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_threshold` = pydatetime.datetime(2050, 1, 1)

Threshold specified in RFC 3280 for switchover from UTCTime to GeneralizedTime.

10.177.1 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`.

10.177.2 Member Function Documentation

10.177.2.1 def rpkisundial.datetime.__add__ (*self*, *y*)

Definition at line 163 of file `sundial.py`.

10.177.2.2 def rpkisundial.datetime.__radd__ (*self*, *y*)

Definition at line 164 of file `sundial.py`.

10.177.2.3 def rpki.sundial.datetime.__rsub__ (*self*, *y*)

Definition at line 165 of file sundial.py.

10.177.2.4 def rpki.sundial.datetime.__str__ (*self*)

Definition at line 124 of file sundial.py.

10.177.2.5 def rpki.sundial.datetime.__sub__ (*self*, *y*)

Definition at line 166 of file sundial.py.

10.177.2.6 def rpki.sundial.datetime.earlier (*self*, *other*)

Return the earlier of two timestamps.

Definition at line 159 of file sundial.py.

10.177.2.7 def rpki.sundial.datetime.from_sql (*cls*, *x*)

Convert from SQL storage format.

Definition at line 136 of file sundial.py.

10.177.2.8 def rpki.sundial.datetime.fromASN1tuple (*cls*, *x*)

Convert from ASN.1 tuple representation.

Definition at line 86 of file sundial.py.

10.177.2.9 def rpkisundial.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`.

10.177.2.10 def rpkisundial.datetime.fromGeneralizedTime (*cls*, *x*)

Convert from ASN.1 GeneralizedTime.

Definition at line 77 of file `sundial.py`.

10.177.2.11 def rpkisundial.datetime.fromUTCTime (*cls*, *x*)

Convert from ASN.1 UTCTime.

Definition at line 68 of file `sundial.py`.

10.177.2.12 def rpkisundial.datetime.fromXMLtime (*cls*, *x*)

Convert from XML time representation.

Definition at line 111 of file `sundial.py`.

10.177.2.13 def rpkisundial.datetime.later (*self*, *other*)

Return the later of two timestamps.

Definition at line 155 of file `sundial.py`.

10.177.2.14 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.

10.177.2.15 def rpki.sundial.datetime.toASN1tuple (*self*)

Convert to ASN.1 tuple representation.

Definition at line 101 of file sundial.py.

10.177.2.16 def rpki.sundial.datetime.toGeneralizedTime (*self*)

Convert to ASN.1 GeneralizedTime.

Definition at line 81 of file sundial.py.

10.177.2.17 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.

10.177.2.18 def rpki.sundial.datetime.toUTCTime (*self*)

Convert to ASN.1 UTCTime.

Definition at line 72 of file sundial.py.

10.177.2.19 def rpki.sundial.datetime.toXMLtime (*self*)

Convert to XML time representation.

Definition at line 120 of file sundial.py.

10.177.3 Member Data Documentation**10.177.3.1 rpki::sundial.datetime::PKIX_threshold =
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.

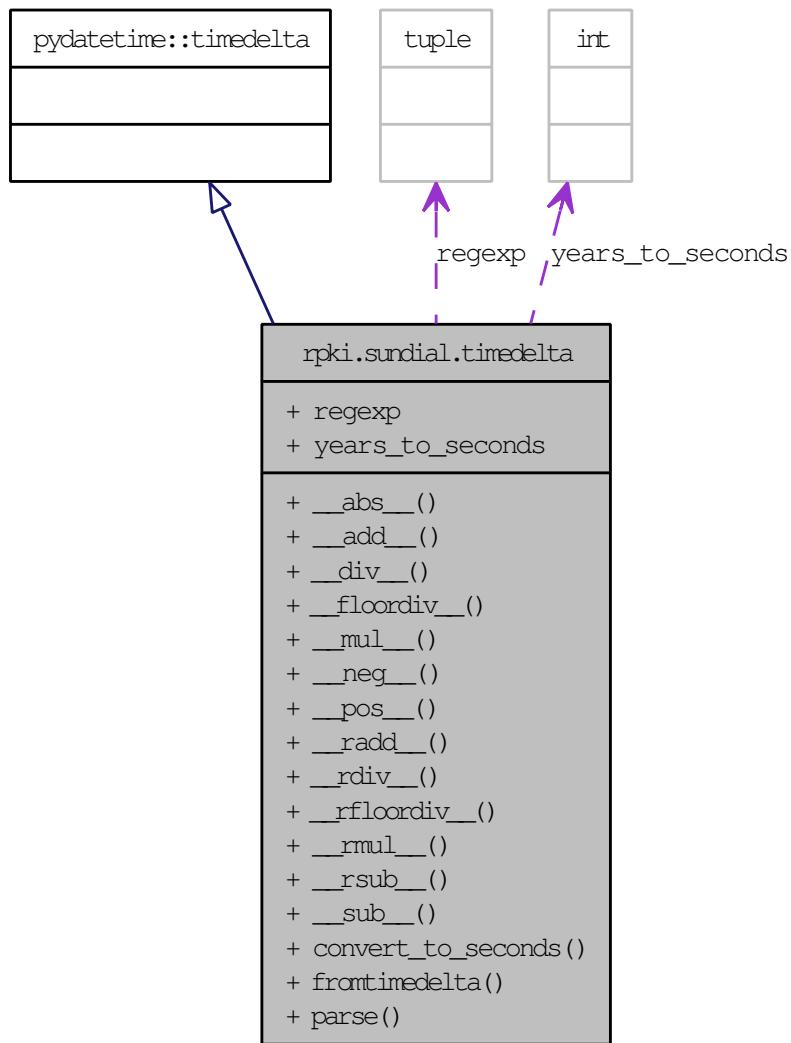
The documentation for this class was generated from the following file:

- [sundial.py \(3191\)](#)

10.178 rpki.sundial.timedelta Class Reference

Inherits [pydatetime::timedelta](#).

Collaboration diagram for rpkisundial.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).

10.178.1 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.

10.178.2 Member Function Documentation**10.178.2.1 def rpkি.sundial.timedelta.__abs__ (*self*)**

Definition at line 243 of file sundial.py.

10.178.2.2 def rpkি.sundial.timedelta.__add__ (*self*, *x*)

Definition at line 244 of file sundial.py.

10.178.2.3 def rpkি.sundial.timedelta.__div__ (*self*, *x*)

Definition at line 245 of file sundial.py.

10.178.2.4 def rpkি.sundial.timedelta.__floordiv__ (*self*, *x*)

Definition at line 246 of file sundial.py.

10.178.2.5 def rpkি.sundial.timedelta.__mul__ (*self*, *x*)

Definition at line 247 of file sundial.py.

10.178.2.6 def rpkি.sundial.timedelta.__neg__ (*self*)

Definition at line 248 of file sundial.py.

10.178.2.7 def rpkি.sundial.timedelta.__pos__ (*self*)

Definition at line 249 of file sundial.py.

10.178.2.8 def rpki.sundial.timedelta.__radd__ (*self*, *x*)

Definition at line 250 of file sundial.py.

10.178.2.9 def rpki.sundial.timedelta.__rdiv__ (*self*, *x*)

Definition at line 251 of file sundial.py.

10.178.2.10 def rpki.sundial.timedelta.__rfloordiv__ (*self*, *x*)

Definition at line 252 of file sundial.py.

10.178.2.11 def rpki.sundial.timedelta.__rmul__ (*self*, *x*)

Definition at line 253 of file sundial.py.

10.178.2.12 def rpki.sundial.timedelta.__rsub__ (*self*, *x*)

Definition at line 254 of file sundial.py.

10.178.2.13 def rpki.sundial.timedelta.__sub__ (*self*, *x*)

Definition at line 255 of file sundial.py.

10.178.2.14 def rpki.sundial.timedelta.convert_to_seconds (*self*)

Convert a timedelta interval to seconds.

Definition at line 234 of file sundial.py.

10.178.2.15 def rpkি.sundial.timedelta.fromtimedelta (*cls*, *x*)

Convert a `datetime.timedelta` object into this subclass.

Definition at line 239 of file `sundial.py`.

10.178.2.16 def rpkি.sundial.timedelta.parse (*cls*, *arg*)

Parse text into a `timedelta` object.

Definition at line 213 of file `sundial.py`.

10.178.3 Member Data Documentation**10.178.3.1 rpkি::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`.

10.178.3.2 rpkি::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:

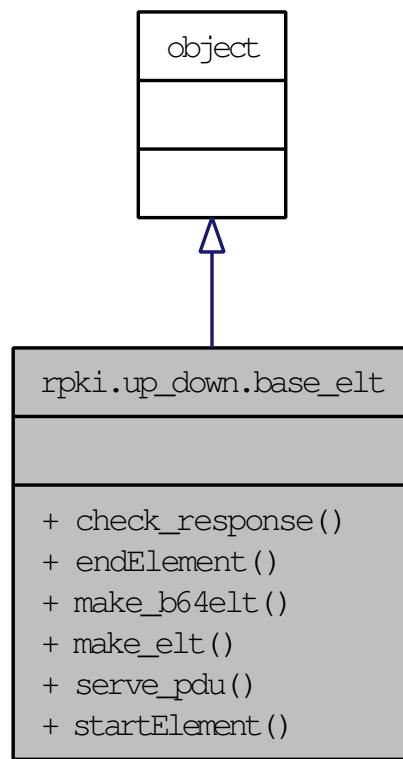
- [sundial.py \(3191\)](#)

10.179 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](#)

10.179.1 Detailed Description

Generic PDU object.

Virtual class, just provides some default methods.

Definition at line 43 of file up_down.py.

10.179.2 Member Function Documentation

10.179.2.1 def rpk.up_down.base_elt.check_response (*self*)

Placeholder for response checking.

Reimplemented in [rpk.up_down.issue_response_pdu](#), and [rpk.up_down.error_response_pdu](#).

Definition at line 91 of file up_down.py.

10.179.2.2 def rpk.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 [rpk.up_down.certificate_elt](#), [rpk.up_down.class_elt](#), [rpk.up_down.issue_pdu](#), and [rpk.up_down.error_response_pdu](#).

Definition at line 59 of file up_down.py.

10.179.2.3 def rpk.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.

10.179.2.4 def rpk.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.

10.179.2.5 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.

10.179.2.6 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.

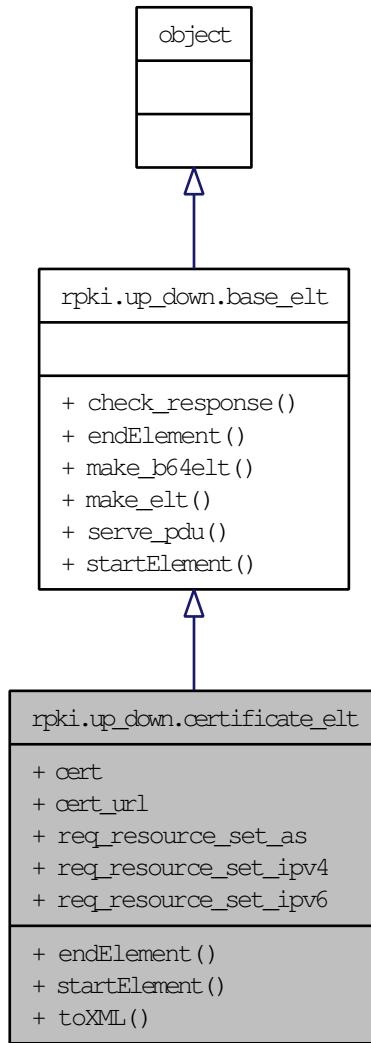
The documentation for this class was generated from the following file:

- [up_down.py \(3162\)](#)

10.180 rpki.up_down.certificate_elt Class Reference

Inherits [rpki::up_down::base_elt](#).

Collaboration diagram for rpk.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](#)

10.180.1 Detailed Description

Up-Down protocol representation of an issued certificate.

Definition at line 128 of file up_down.py.

10.180.2 Member Function Documentation

10.180.2.1 def rpk.up_down.certificate_elt.endElement (*self, stack, name, text*)

Handle *text* content of a <certificate/> element.

Reimplemented from [rpk.up_down.base_elt](#).

Definition at line 143 of file up_down.py.

10.180.2.2 def rpk.up_down.certificate_elt.startElement (*self, stack, name, attrs*)

Handle attributes of <certificate/> element.

Reimplemented from [rpk.up_down.base_elt](#).

Definition at line 133 of file up_down.py.

10.180.2.3 def rpk.up_down.certificate_elt.toXML (*self*)

Generate a <certificate/> element.

Definition at line 151 of file up_down.py.

10.180.3 Member Data Documentation**10.180.3.1 rpki.up_down.certificate_elt.cert**

Definition at line 148 of file up_down.py.

10.180.3.2 rpki.up_down.certificate_elt.cert_url

Definition at line 138 of file up_down.py.

10.180.3.3 rpki.up_down.certificate_elt.req_resource_set_as

Definition at line 139 of file up_down.py.

10.180.3.4 rpki.up_down.certificate_elt.req_resource_set_ipv4

Definition at line 140 of file up_down.py.

10.180.3.5 rpki.up_down.certificate_elt.req_resource_set_ipv6

Definition at line 141 of file up_down.py.

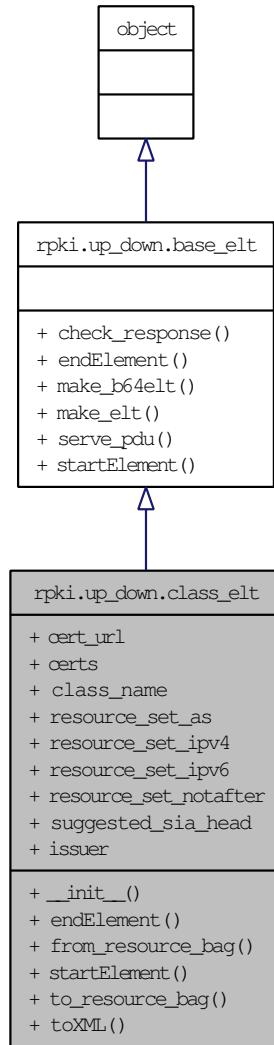
The documentation for this class was generated from the following file:

- [up_down.py \(3162\)](#)

10.181 rpki.up_down.class_elt Class Reference

Inherits [rpki::up_down::base_elt](#).

Collaboration diagram for rpk.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

10.181.1 Detailed Description

Up-Down protocol representation of a resource class.

Definition at line 160 of file up_down.py.

10.181.2 Member Function Documentation

10.181.2.1 def rpk.up_down.class_elt.__init__ (self)

Initialize class_elt.

Definition at line 167 of file up_down.py.

10.181.2.2 def rpk.up_down.class_elt.endElement (self, stack, name, text)

Handle <class/> elements and their children.

Reimplemented from [rpk.up_down.base_elt](#).

Definition at line 191 of file up_down.py.

10.181.2.3 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.

10.181.2.4 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.

10.181.2.5 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.

10.181.2.6 def rpki.up_down.class_elt.toXML (self)

Generate a <class/> element.

Definition at line 201 of file up_down.py.

10.181.3 Member Data Documentation**10.181.3.1 rpki.up_down.class_elt.cert_url**

Definition at line 184 of file up_down.py.

10.181.3.2 rpki.up_down.class_elt.certs

Definition at line 170 of file up_down.py.

10.181.3.3 rpki.up_down.class_elt.class_name

Definition at line 183 of file up_down.py.

10.181.3.4 rpki.up_down.class_elt.issuer = None [static]

Definition at line 165 of file up_down.py.

10.181.3.5 rpki.up_down.class_elt.resource_set_as

Definition at line 186 of file up_down.py.

10.181.3.6 rpki.up_down.class_elt.resource_set_ipv4

Definition at line 187 of file up_down.py.

10.181.3.7 rpki.up_down.class_elt.resource_set_ipv6

Definition at line 188 of file up_down.py.

10.181.3.8 rpki.up_down.class_elt.resource_set_notafter

Definition at line 189 of file up_down.py.

10.181.3.9 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:

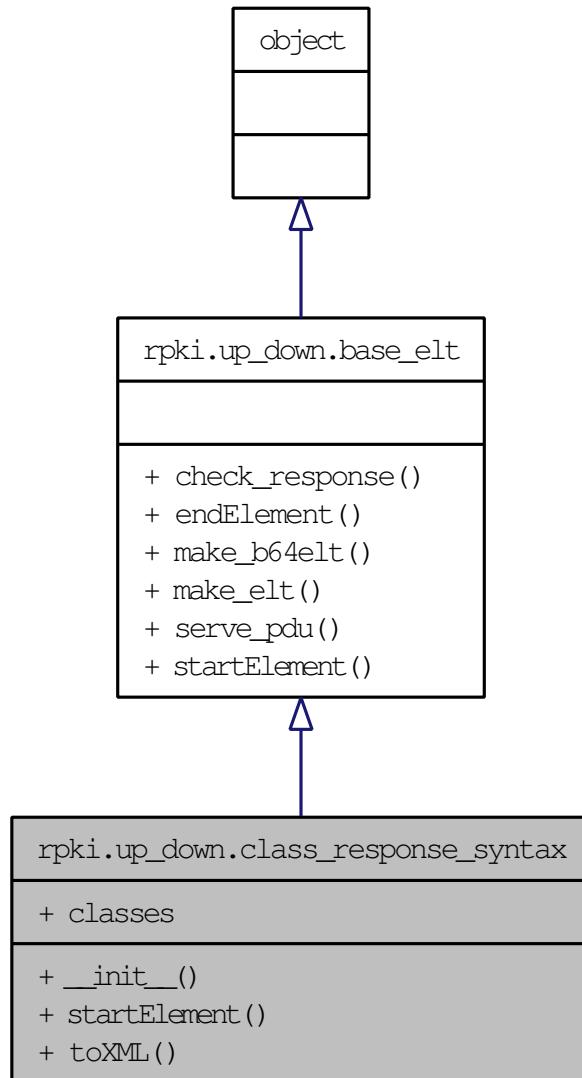
- [up_down.py \(3162\)](#)

10.182 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](#)

10.182.1 Detailed Description

Syntax for Up-Down protocol "list_response" and "issue_response" PDUs.

Definition at line 285 of file up_down.py.

10.182.2 Member Function Documentation

10.182.2.1 def rpk.up_down.class_response_syntax.__init__ (*self*)

Initialize class_response_syntax.

Definition at line 290 of file up_down.py.

10.182.2.2 def rpk.up_down.class_response_syntax.startElement (*self, stack, name, attrs*)

Handle "list_response" and "issue_response" PDUs.

Reimplemented from [rpk.up_down.base_elt](#).

Definition at line 297 of file up_down.py.

10.182.2.3 def rpk.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.

10.182.3 Member Data Documentation

10.182.3.1 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:

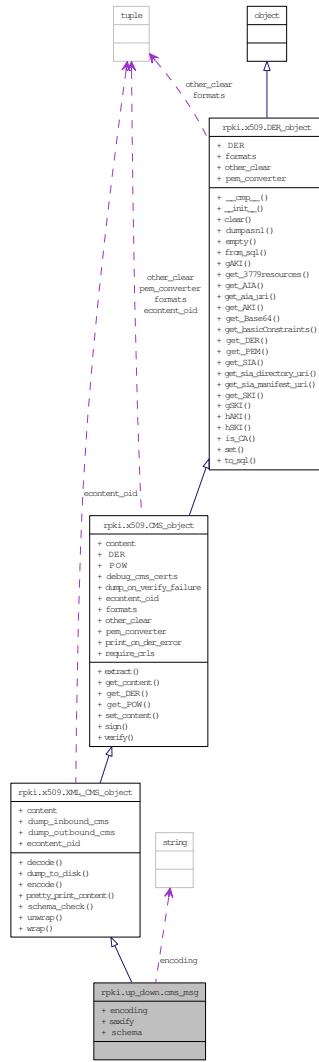
- [up_down.py \(3162\)](#)

10.183 rpki.up_down.cms_msg Class Reference

Inherits [rpki::x509::XML_CMS_object](#).

Inherited by [rootd.cms_msg](#).

Collaboration diagram for rpk.up_down.cms_msg:



Static Public Attributes

- string `encoding` = "UTF-8"
- `saxify` = `sax_handler.saxify`
- `schema` = `rpk.relaxng.up_down`

10.183.1 Detailed Description

Class to hold a CMS-signed up-down PDU.

Definition at line 685 of file up_down.py.

10.183.2 Member Data Documentation

10.183.2.1 string rpki.up_down.cms_msg.encoding = "UTF-8" [static]

Definition at line 690 of file up_down.py.

10.183.2.2 rpki.up_down.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented in [rootd.cms_msg](#).

Definition at line 692 of file up_down.py.

10.183.2.3 rpki.up_down.cms_msg.schema = rpki.relaxng.up_down [static]

Definition at line 691 of file up_down.py.

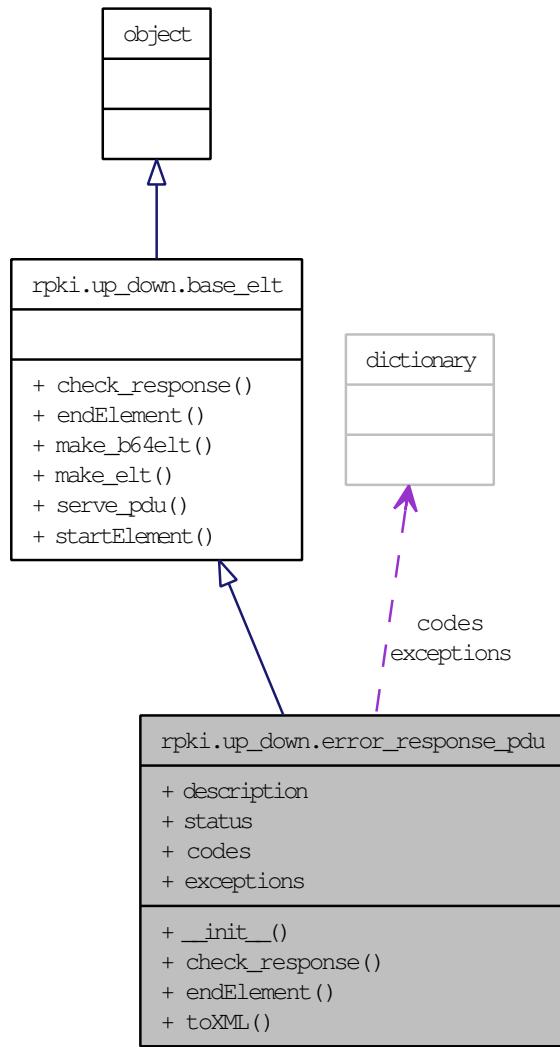
The documentation for this class was generated from the following file:

- [up_down.py \(3162\)](#)

10.184 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](#)

10.184.1 Detailed Description

Up-Down protocol "error_response" PDU.

Definition at line 505 of file up_down.py.

10.184.2 Member Function Documentation

10.184.2.1 def rpk.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.

10.184.2.2 def rpk.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 [rpk.up_down.base_elt](#).

Definition at line 564 of file up_down.py.

10.184.2.3 def rpk.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.

10.184.2.4 def rpki.up_down.error_response_pdu.toXML (*self*)

Generate payload of "error_response" PDU.

Definition at line 549 of file up_down.py.

10.184.3 Member Data Documentation

10.184.3.1 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.

10.184.3.2 rpki.up_down.error_response_pdu.description

Definition at line 531 of file up_down.py.

10.184.3.3 dictionary rpki.up_down.error_response_pdu.exceptions [static]

Initial value:

```
{  
    rpki.exceptions.NoActiveCA : 1202 }
```

Definition at line 521 of file up_down.py.

10.184.3.4 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:

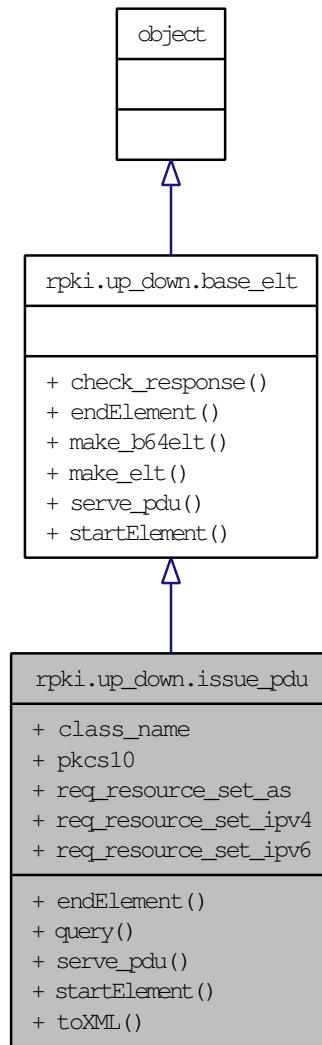
- [up_down.py \(3162\)](#)

10.185 rpki.up_down.issue_pdu Class Reference

Inherits [rpki::up_down::base_elt](#).

Inherited by [rootd.issue_pdu](#).

Collaboration diagram for rpk.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](#)

10.185.1 Detailed Description

Up-Down protocol "issue" PDU.

Definition at line 317 of file up_down.py.

10.185.2 Member Function Documentation

10.185.2.1 def rpk.up_down.issue_pdu.endElement (*self, stack, name, text*)

Handle "issue" PDU.

Reimplemented from [rpk.up_down.base_elt](#).

Definition at line 332 of file up_down.py.

10.185.2.2 def rpk.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.

10.185.2.3 def rpk.up_down.issue_pdu.serve_pdu (*self, q_msg, r_msg, child, callback, errback*)

Serve one issue request PDU.

Reimplemented from [rpk.up_down.base_elt](#).

Reimplemented in [rootd.issue_pdu](#).

Definition at line 349 of file up_down.py.

10.185.2.4 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.

10.185.2.5 def rpki.up_down.issue_pdu.toXML (*self*)

Generate payload of "issue" PDU.

Definition at line 340 of file up_down.py.

10.185.3 Member Data Documentation**10.185.3.1 rpki.up_down.issue_pdu.class_name**

Definition at line 327 of file up_down.py.

10.185.3.2 rpki.up_down.issue_pdu.pkcs10

Definition at line 337 of file up_down.py.

10.185.3.3 rpki.up_down.issue_pdu.req_resource_set_as

Definition at line 328 of file up_down.py.

10.185.3.4 rpki.up_down.issue_pdu.req_resource_set_ipv4

Definition at line 329 of file up_down.py.

10.185.3.5 rpki.up_down.issue_pdu.req_resource_set_ipv6

Definition at line 330 of file up_down.py.

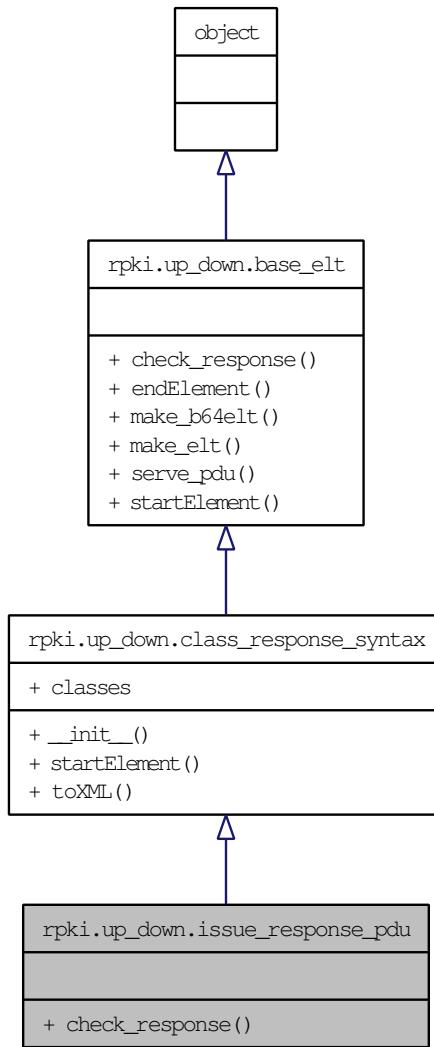
The documentation for this class was generated from the following file:

- [up_down.py \(3162\)](#)

10.186 rpki.up_down.issue_response_pdu Class Reference

Inherits [rpki::up_down::class_response_syntax](#).

Collaboration diagram for rpk.up_down.issue_response_pdu:



Public Member Functions

- def [check_response](#)

10.186.1 Detailed Description

Up-Down protocol "issue_response" PDU.

Definition at line 431 of file up_down.py.

10.186.2 Member Function Documentation

10.186.2.1 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:

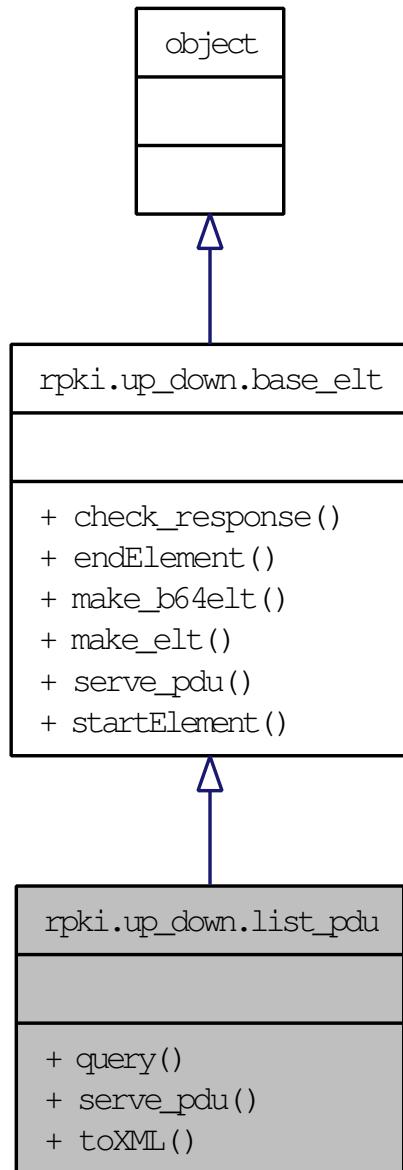
- [up_down.py \(3162\)](#)

10.187 rpki.up_down.list_pdu Class Reference

Inherits [rpki::up_down::base_elt](#).

Inherited by [rootd.list_pdu](#).

Collaboration diagram for rpk.up_down.list_pdu:



Public Member Functions

- def [query](#)

- def [serve_pdu](#)
- def [toXML](#)

10.187.1 Detailed Description

Up-Down protocol "list" PDU.

Definition at line 231 of file up_down.py.

10.187.2 Member Function Documentation

10.187.2.1 def rpk.up_down.list_pdu.query (*cls, parent, cb, eb*)

Send a "list" query to parent.

Definition at line 273 of file up_down.py.

10.187.2.2 def rpk.up_down.list_pdu.serve_pdu (*self, q_msg, r_msg, child, callback, errback*)

Serve one "list" PDU.

Reimplemented from [rpk.up_down.base_elt](#).

Reimplemented in [rootd.list_pdu](#).

Definition at line 240 of file up_down.py.

10.187.2.3 def rpk.up_down.list_pdu.toXML (*self*)

Generate (empty) payload of "list" PDU.

Definition at line 236 of file up_down.py.

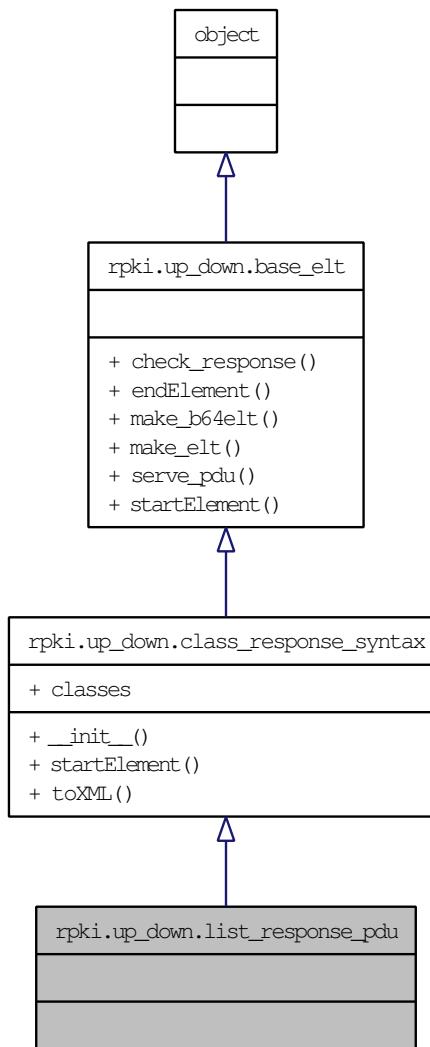
The documentation for this class was generated from the following file:

- [up_down.py \(3162\)](#)

10.188 rpk.up_down.list_response_pdu Class Reference

Inherits [rpk::up_down::class_response_syntax](#).

Collaboration diagram for rpk.up_down.list_response_pdu:



10.188.1 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:

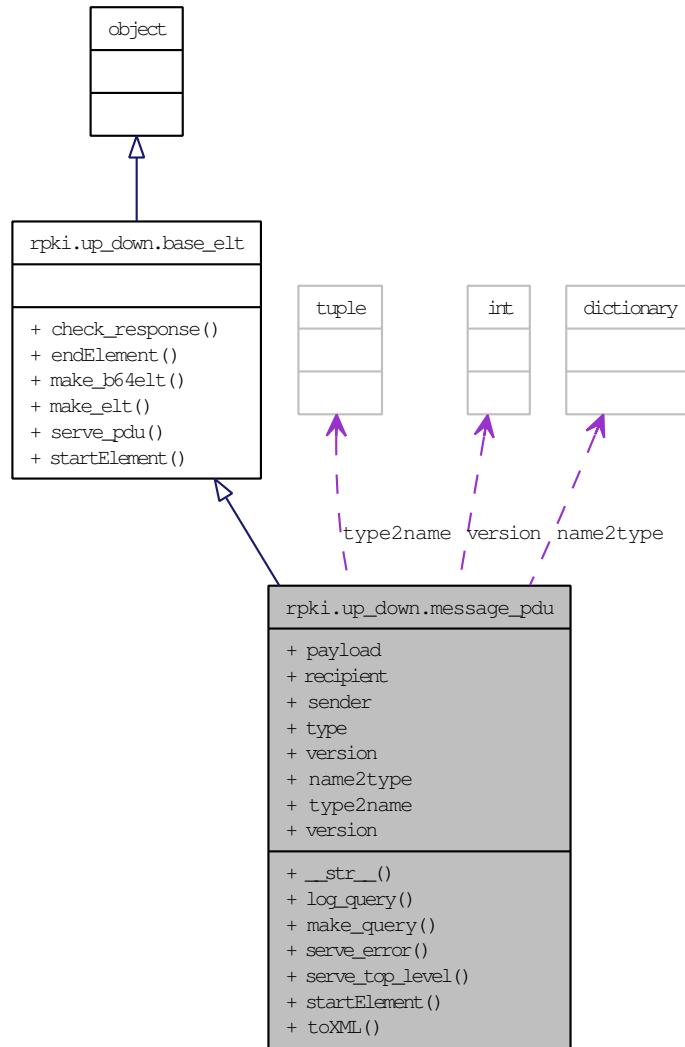
- [up_down.py \(3162\)](#)

10.189 rpkid.up_down.message_pdu Class Reference

Inherits [rpki::up_down::base_elt](#).

Inherited by [rootd.message_pdu](#).

Collaboration diagram for rpk.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

10.189.1 Detailed Description

Up-Down protocol message wrapper PDU.

Definition at line 571 of file up_down.py.

10.189.2 Member Function Documentation

10.189.2.1 def rpk.up_down.message_pdu.[__str__](#) (*self*)

Convert a message PDU to a string.

Definition at line 613 of file up_down.py.

10.189.2.2 def rpk.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.

10.189.2.3 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.

10.189.2.4 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.

10.189.2.5 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.

10.189.2.6 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.

10.189.2.7 def rpki.up_down.message_pdu.toXML (*self*)

Generate payload of message PDU.

Definition at line 589 of file up_down.py.

10.189.3 Member Data Documentation

10.189.3.1 dictionary rpkid.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.

10.189.3.2 rpkid.up_down.message_pdu.payload

Definition at line 610 of file up_down.py.

10.189.3.3 rpkid.up_down.message_pdu.recipient

Definition at line 608 of file up_down.py.

10.189.3.4 rpkid.up_down.message_pdu.sender

Definition at line 607 of file up_down.py.

10.189.3.5 rpkid.up_down.message_pdu.type

Definition at line 609 of file up_down.py.

10.189.3.6 tuple rpkid.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.

10.189.3.7 rpki.up_down.message_pdu.version

Definition at line 606 of file up_down.py.

10.189.3.8 int rpki.up_down.message_pdu.version = 1 [static]

Definition at line 576 of file up_down.py.

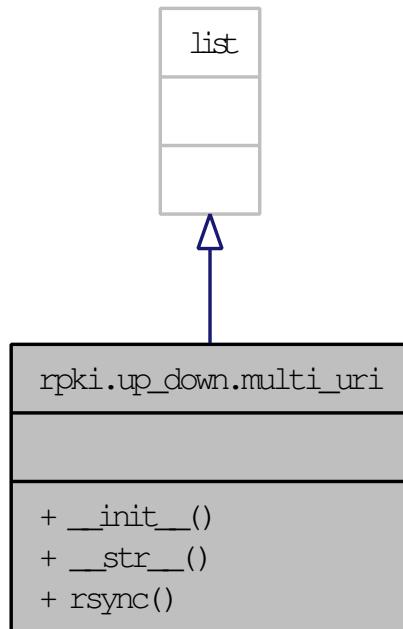
The documentation for this class was generated from the following file:

- [up_down.py \(3162\)](#)

10.190 rpki.up_down.multi_uri Class Reference

Inherits list.

Collaboration diagram for rpk.up_down.multi_uri:



Public Member Functions

- def [__init__](#)
- def [__str__](#)
- def [rsync](#)

10.190.1 Detailed Description

Container for a set of URIs.

Definition at line 95 of file up_down.py.

10.190.2 Member Function Documentation

10.190.2.1 def rpk.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.

10.190.2.2 def rpkি.up_down.multi_uri.__str__ (self)

Convert a multi_uri back to a string representation.

Definition at line 115 of file up_down.py.

10.190.2.3 def rpkি.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:

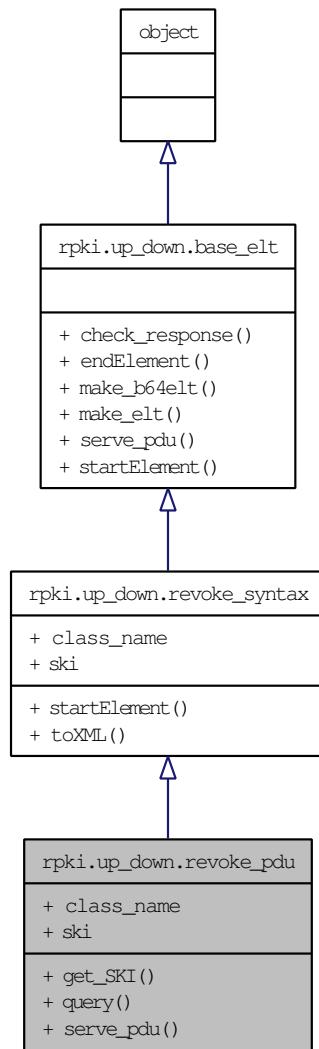
- [up_down.py \(3162\)](#)

10.191 rpkি.up_down.revoke_pdu Class Reference

Inherits [rpkি::up_down::revoke_syntax](#).

Inherited by [rootd.revoke_pdu](#).

Collaboration diagram for rpk.up_down.revoke_pdu:



Public Member Functions

- def [get_SKI](#)
- def [query](#)
- def [serve_pdu](#)

Public Attributes

- `class_name`
- `ski`

10.191.1 Detailed Description

Up-Down protocol "revoke" PDU.

Definition at line 458 of file up_down.py.

10.191.2 Member Function Documentation

10.191.2.1 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.

10.191.2.2 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.

10.191.2.3 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.

10.191.3 Member Data Documentation**10.191.3.1 rpki.up_down.revoke_pdu.class_name**

Reimplemented from [rpki.up_down.revoke_syntax](#).

Definition at line 493 of file `up_down.py`.

10.191.3.2 rpki.up_down.revoke_pdu.ski

Reimplemented from [rpki.up_down.revoke_syntax](#).

Definition at line 494 of file `up_down.py`.

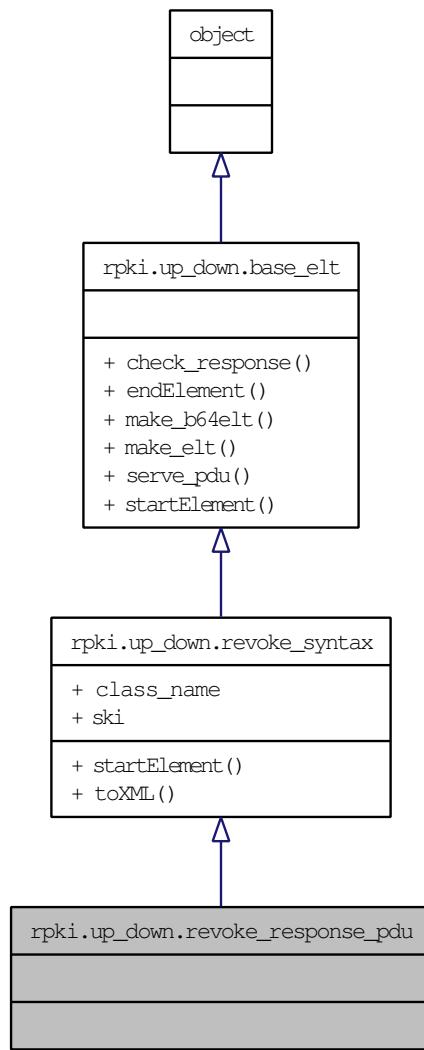
The documentation for this class was generated from the following file:

- [up_down.py \(3162\)](#)

10.192 rpki.up_down.revoke_response_pdu Class Reference

Inherits [rpki::up_down::revoke_syntax](#).

Collaboration diagram for rpk.up_down.revocate_response_pdu:



10.192.1 Detailed Description

Up-Down protocol "revocate_response" PDU.

Definition at line 498 of file `up_down.py`.

The documentation for this class was generated from the following file:

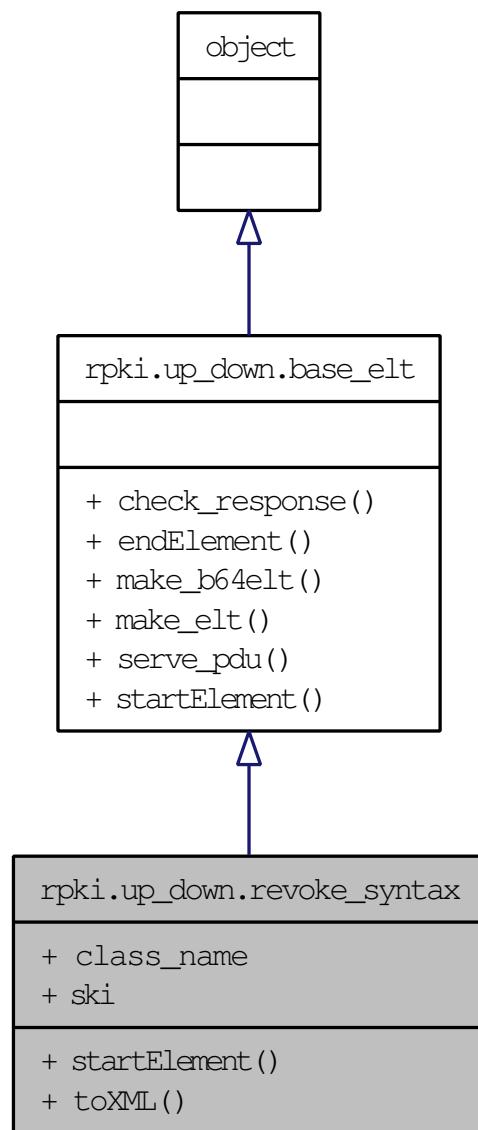
- [up_down.py \(3162\)](#)

10.193 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](#)

10.193.1 Detailed Description

Syntax for Up-Down protocol "revocate" and "revocate_response" PDUs.

Definition at line 444 of file up_down.py.

10.193.2 Member Function Documentation

10.193.2.1 def rpki.up_down.revocate_syntax.startElement (*self*, *stack*, *name*, *attrs*)

Handle "revocate" PDU.

Reimplemented from [rpki.up_down.base_elt](#).

Definition at line 449 of file up_down.py.

10.193.2.2 def rpki.up_down.revocate_syntax.toXML (*self*)

Generate payload of "revocate" PDU.

Definition at line 454 of file up_down.py.

10.193.3 Member Data Documentation

10.193.3.1 rpki.up_down.revocate_syntax.class_name

Reimplemented in [rpki.up_down.revocate_pdu](#).

Definition at line 451 of file up_down.py.

10.193.3.2 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:

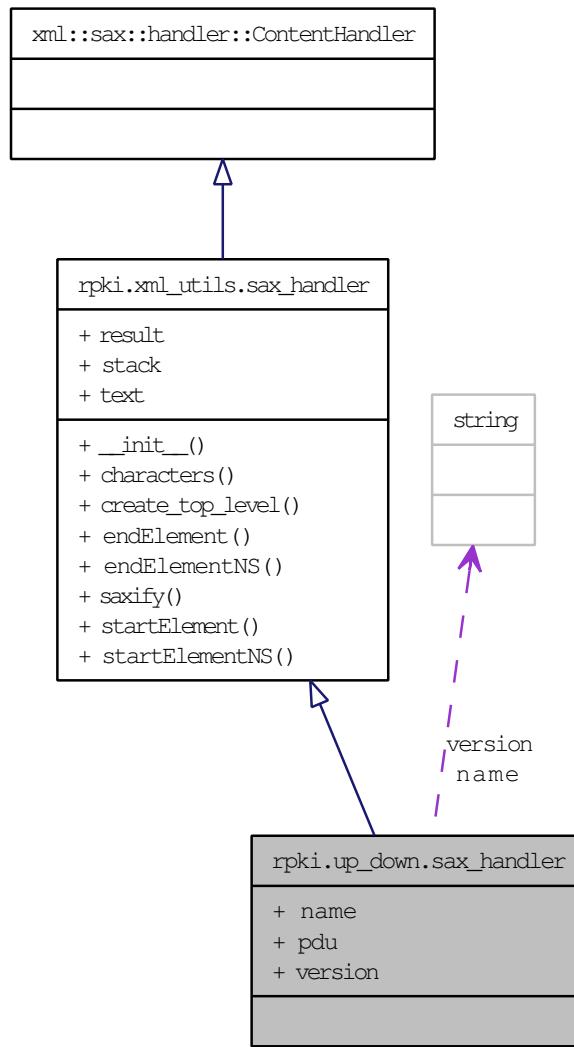
- [up_down.py \(3162\)](#)

10.194 rpki.up_down.sax_handler Class Reference

Inherits [rpki::xml_utils::sax_handler](#).

Inherited by [rootd.sax_handler](#).

Collaboration diagram for rpk.up_down.sax_handler:



Static Public Attributes

- string `name` = "message"
- `pdu` = `message_pdu`
- string `version` = "1"

10.194.1 Detailed Description

SAX handler for Up-Down protocol.

Definition at line 676 of file up_down.py.

10.194.2 Member Data Documentation

10.194.2.1 string rpki.up_down.sax_handler.name = "message" [static]

Definition at line 682 of file up_down.py.

10.194.2.2 rpki.up_down.sax_handler.pdu = message_pdu [static]

Reimplemented in [rootd.sax_handler](#).

Definition at line 681 of file up_down.py.

10.194.2.3 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:

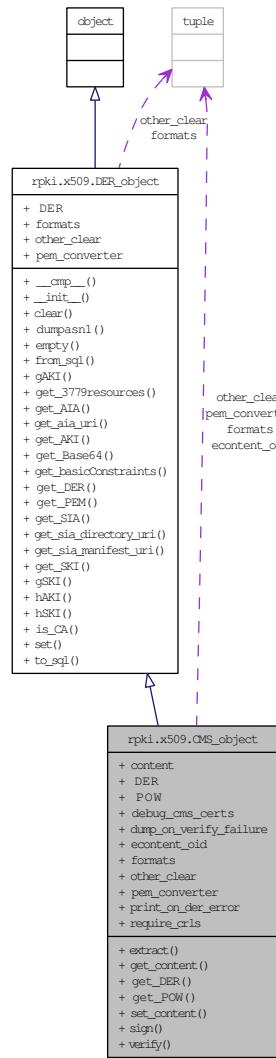
- [up_down.py \(3162\)](#)

10.195 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 rpkix509.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.

10.195.1 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 handled via separate methods.

Definition at line 735 of file x509.py.

10.195.2 Member Function Documentation

10.195.2.1 def rpkix509.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.

10.195.2.2 def rpkix509.CMS_object.get_content (*self*)

Get the inner content of this CMS_object.

Definition at line 797 of file x509.py.

10.195.2.3 def rpkix509.CMS_object.get_DER (*self*)

Get the DER value of this CMS_object.

Reimplemented from [rpkix509.DER_object](#).

Definition at line 776 of file x509.py.

10.195.2.4 def rpkix509.CMS_object.get_POW (*self*)

Get the POW value of this CMS_object.

Definition at line 788 of file x509.py.

10.195.2.5 def rpkix509.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.

10.195.2.6 def rpkix509.CMS_object.sign (*self, keypair, certs, crls = None, no_certs = False*)

Sign and wrap inner content.

Definition at line 914 of file x509.py.

10.195.2.7 def rpkix509.CMS_object.verify (*self, ta*)

Verify CMS wrapper and store inner content.

Definition at line 812 of file x509.py.

10.195.3 Member Data Documentation**10.195.3.1 rpkix509.CMS_object.content**

Reimplemented in [rpkix509.DER_CMS_object](#), and [rpkix509.XML_CMS_object](#).

Definition at line 810 of file x509.py.

10.195.3.2 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.

10.195.3.3 rpki.x509.CMS_object.DER

DER value of this object.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 784 of file x509.py.

10.195.3.4 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.

10.195.3.5 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.

10.195.3.6 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.

10.195.3.7 tuple rpkix509.CMS_object.other_clear = ('content',) [static]

Other attributes that self.clear() should whack.

Reimplemented from [rpkix509.DER_object](#).

Definition at line 749 of file x509.py.

10.195.3.8 tuple rpkix509.CMS_object.pem_converter = PEM_converter("CMS") [static]

PEM converter for this object.

Reimplemented from [rpkix509.DER_object](#).

Reimplemented in [rpkix509.SignedManifest](#), and [rpkix509.ROA](#).

Definition at line 751 of file x509.py.

10.195.3.9 rpkix509.CMS_object.POW

Definition at line 794 of file x509.py.

10.195.3.10 rpkix509.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.

10.195.3.11 rpkix509.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 unconditionally mandatory in such cases.

Definition at line 768 of file x509.py.

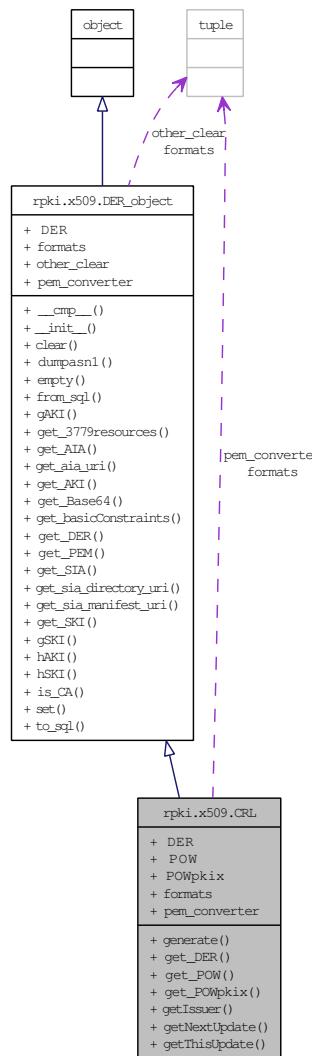
The documentation for this class was generated from the following file:

- [x509.py \(3107\)](#)

10.196 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.

10.196.1 Detailed Description

Class to hold a Certificate Revocation List.

Definition at line 1140 of file x509.py.

10.196.2 Member Function Documentation

10.196.2.1 def rpkix.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.

10.196.2.2 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.

10.196.2.3 def rpki.x509.CRL.get_POW (*self*)

Get the POW value of this CRL.

Definition at line 1163 of file x509.py.

10.196.2.4 def rpki.x509.CRL.get_POWpkix (*self*)

Get the POW.pkix value of this CRL.

Definition at line 1172 of file x509.py.

10.196.2.5 def rpki.x509.CRL.getIssuer (*self*)

Get issuer value of this CRL.

Definition at line 1191 of file x509.py.

10.196.2.6 def rpki.x509.CRL.getNextUpdate (*self*)

Get nextUpdate value from this CRL.

Definition at line 1187 of file x509.py.

10.196.2.7 def rpki.x509.CRL.getThisUpdate (*self*)

Get thisUpdate value from this CRL.

Definition at line 1183 of file x509.py.

10.196.3 Member Data Documentation**10.196.3.1 rpki.x509.CRL.DER**

DER value of this object.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 1156 of file x509.py.

10.196.3.2 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.

10.196.3.3 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.

10.196.3.4 rpki.x509.CRL.POW

Definition at line 1169 of file x509.py.

10.196.3.5 rpki.x509.CRL.PO Wpkix

Definition at line 1180 of file x509.py.

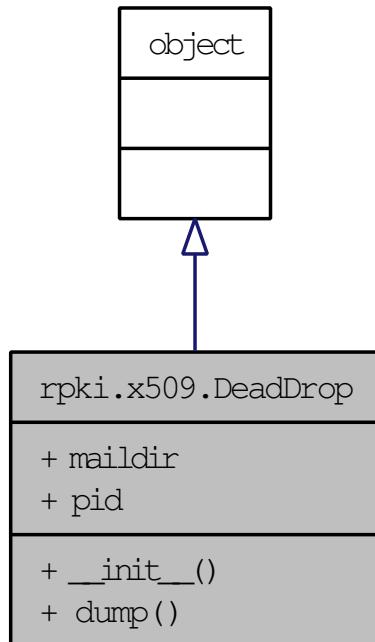
The documentation for this class was generated from the following file:

- [x509.py \(3107\)](#)

10.197 rpki.x509.DeadDrop Class Reference

Inherits [object](#).

Collaboration diagram for rpki.x509.DeadDrop:



Public Member Functions

- def [__init__](#)
- def [dump](#)

Public Attributes

- [maildir](#)
- [pid](#)

10.197.1 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.

10.197.2 Member Function Documentation

10.197.2.1 def rPKI.x509.DeadDrop.__init__ (*self, name*)

Definition at line 1043 of file x509.py.

10.197.2.2 def rPKI.x509.DeadDrop.dump (*self, obj*)

Definition at line 1047 of file x509.py.

10.197.3 Member Data Documentation

10.197.3.1 rPKI.x509.DeadDrop.maildir

Definition at line 1044 of file x509.py.

10.197.3.2 rPKI.x509.DeadDrop.pid

Definition at line 1045 of file x509.py.

The documentation for this class was generated from the following file:

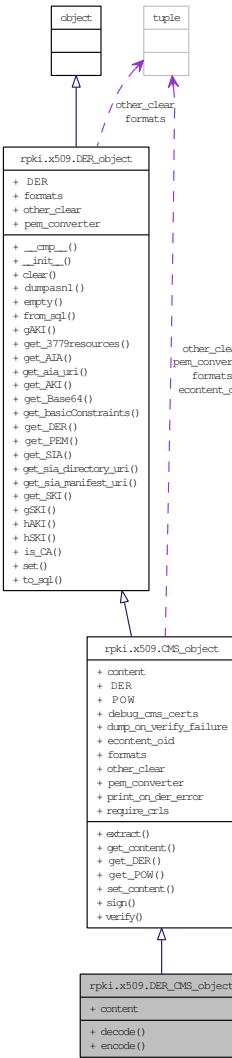
- [x509.py \(3107\)](#)

10.198 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](#)

10.198.1 Detailed Description

Class to hold CMS objects with DER-based content.

Definition at line 950 of file x509.py.

10.198.2 Member Function Documentation

10.198.2.1 def rpki.x509.DER_CMS_object.decode (*self, der*)

Decode DER and set inner content.

Definition at line 959 of file x509.py.

10.198.2.2 def rpki.x509.DER_CMS_object.encode (*self*)

Encode inner content for signing.

Definition at line 955 of file x509.py.

10.198.3 Member Data Documentation

10.198.3.1 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:

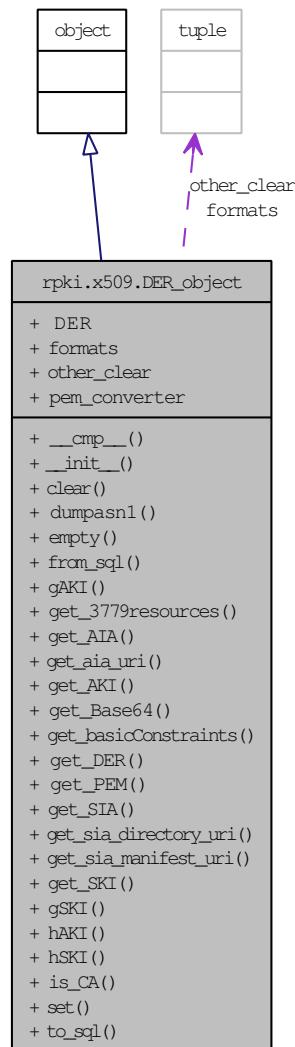
- [x509.py \(3107\)](#)

10.199 rpkix509.DER_object Class Reference

Inherits [object](#).

Inherited by [rpkix509.CMS_object](#), [rpkix509.CRL](#), [rpkix509.PKCS10](#), [rpkix509.RSA](#), [rpkix509.RSApublic](#), and [rpkix509.X509](#).

Collaboration diagram for rpkix509.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.

10.199.1 Detailed Description

Virtual class to hold a generic DER object.

Definition at line 117 of file x509.py.

10.199.2 Member Function Documentation

10.199.2.1 def rpkix509.DER_object.__cmp__ (*self, other*)

Compare two DER-encoded objects.

Definition at line 212 of file x509.py.

10.199.2.2 def rpkix509.DER_object.__init__ (*self, kw*)

Initialize a DER_object.

Definition at line 150 of file x509.py.

10.199.2.3 def rpkix509.DER_object.clear (*self*)

Make this object empty.

Definition at line 143 of file x509.py.

10.199.2.4 def rpkix509.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.

10.199.2.5 def rpki.x509.DER_object.empty (*self*)

Test whether this object is empty.

Definition at line 134 of file x509.py.

10.199.2.6 def rpki.x509.DER_object.from_sql (*cls*, *x*)

Convert from SQL storage format.

Definition at line 333 of file x509.py.

10.199.2.7 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.

10.199.2.8 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.

10.199.2.9 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.

10.199.2.10 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.

10.199.2.11 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.

10.199.2.12 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.

10.199.2.13 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.

10.199.2.14 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.

10.199.2.15 def rpki.x509.DER_object.get_PEM (*self*)

Get the PEM representation of this object.

Definition at line 208 of file x509.py.

10.199.2.16 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.

10.199.2.17 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.

10.199.2.18 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.

10.199.2.19 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.

10.199.2.20 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.

10.199.2.21 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.

10.199.2.22 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.

10.199.2.23 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.

10.199.2.24 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.

10.199.2.25 def rpki.x509.DER_object.to_sql (*self*)

Convert to SQL storage format.

Definition at line 337 of file x509.py.

10.199.3 Member Data Documentation**10.199.3.1 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.

10.199.3.2 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.

10.199.3.3 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.

10.199.3.4 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](#).

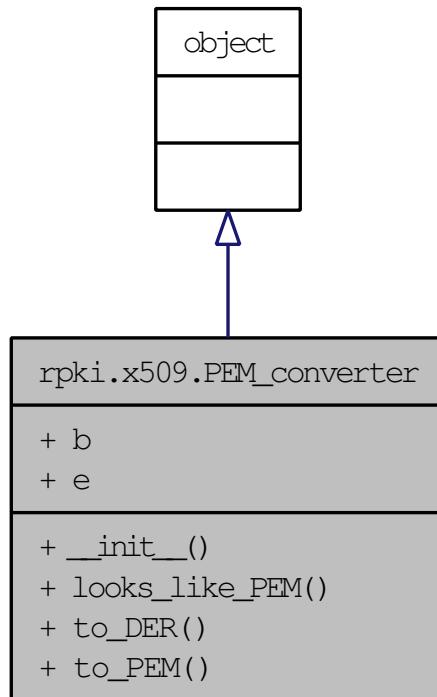
The documentation for this class was generated from the following file:

- [x509.py \(3107\)](#)

10.200 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](#)

10.200.1 Detailed Description

Convert between DER and PEM encodings for various kinds of ASN.1 data.

Definition at line 62 of file x509.py.

10.200.2 Member Function Documentation

10.200.2.1 def rpkix509.PEM_converter.__init__ (*self*, *kind*)

Initialize PEM_converter.

Definition at line 67 of file x509.py.

10.200.2.2 def rpkix509.PEM_converter.looks_like_PEM (*self*, *text*)

Guess whether text looks like a PEM encoding.

Definition at line 74 of file x509.py.

10.200.2.3 def rpkix509.PEM_converter.to_DER (*self*, *pem*)

Convert from PEM to DER.

Definition at line 81 of file x509.py.

10.200.2.4 def rpki.x509.PEM_converter.to_PEM (*self*, *der*)

Convert from DER to PEM.

Definition at line 94 of file x509.py.

10.200.3 Member Data Documentation**10.200.3.1 rpki.x509.PEM_converter.b**

Definition at line 71 of file x509.py.

10.200.3.2 rpki.x509.PEM_converter.e

Definition at line 72 of file x509.py.

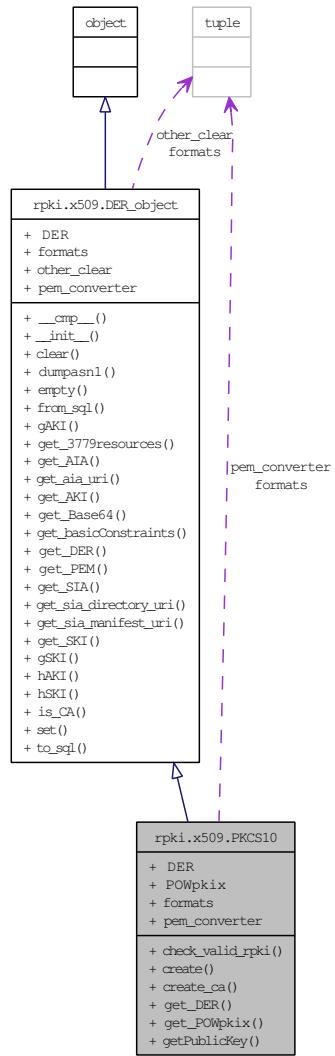
The documentation for this class was generated from the following file:

- [x509.py \(3107\)](#)

10.201 rpki.x509.PKCS10 Class Reference

Inherits [rpki::x509::DER_object](#).

Collaboration diagram for rpkix509.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.

10.201.1 Detailed Description

Class to hold a PKCS #10 request.

Definition at line 534 of file x509.py.

10.201.2 Member Function Documentation

10.201.2.1 def rpkix509.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.

10.201.2.2 def rpkix509.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.

10.201.2.3 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.

10.201.2.4 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.

10.201.2.5 def rpki.x509.PKCS10.get_POWpkix (*self*)

Get the POW.pkix value of this certification request.

Definition at line 554 of file x509.py.

10.201.2.6 def rpki.x509.PKCS10.getPublicKey (*self*)

Extract the public key from this certification request.

Definition at line 565 of file x509.py.

10.201.3 Member Data Documentation**10.201.3.1 rpki.x509.PKCS10.DER**

DER value of this object.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 550 of file x509.py.

10.201.3.2 tuple rpkix509.PKCS10.formats = ("DER", "POWpkix") [static]

Formats supported in this object.

Reimplemented from [rpkix509.DER_object](#).

Definition at line 539 of file x509.py.

10.201.3.3 tuple rpkix509.PKCS10.pem_converter = PEM_converter("CERTIFICATE REQUEST") [static]

PEM converter for this object.

Reimplemented from [rpkix509.DER_object](#).

Definition at line 540 of file x509.py.

10.201.3.4 rpkix509.PKCS10.POWpkix

Definition at line 562 of file x509.py.

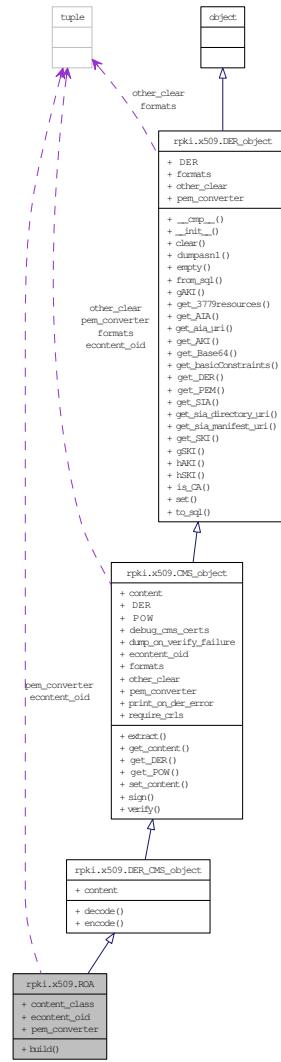
The documentation for this class was generated from the following file:

- [x509.py \(3107\)](#)

10.202 rpkix509.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.

10.202.1 Detailed Description

Class to hold a signed ROA.

Definition at line 1007 of file x509.py.

10.202.2 Member Function Documentation

10.202.2.1 `def rpki.x509.ROA.build (cls, asn, ipv4, ipv6, keypair, certs, version = 0)`

Build a ROA.

Definition at line 1017 of file x509.py.

10.202.3 Member Data Documentation

10.202.3.1 `rpki.x509.ROA.content_class = rpki.roa.RouteOriginAttestation [static]`

Definition at line 1013 of file x509.py.

10.202.3.2 `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.

10.202.3.3 `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](#).

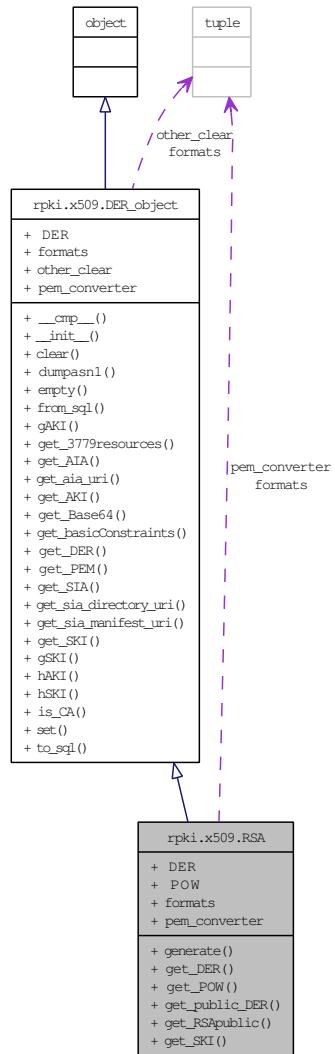
The documentation for this class was generated from the following file:

- [x509.py \(3107\)](#)

10.203 rpki.x509.RSA Class Reference

Inherits [rpki::x509::DER_object](#).

Collaboration diagram for rpkix509.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.

10.203.1 Detailed Description

Class to hold an RSA key pair.

Definition at line 643 of file x509.py.

10.203.2 Member Function Documentation

10.203.2.1 def rpkix509.RSA.generate (*cls, keylength = 2048*)

Generate a new keypair.

Definition at line 673 of file x509.py.

10.203.2.2 def rpkix509.RSA.get_DER (*self*)

Get the DER value of this keypair.

Reimplemented from [rpkix509.DER_object](#).

Definition at line 651 of file x509.py.

10.203.2.3 def rpki.x509.RSA.get_POW (*self*)

Get the POW value of this keypair.

Definition at line 663 of file x509.py.

10.203.2.4 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.

10.203.2.5 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.

10.203.2.6 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.

10.203.3 Member Data Documentation**10.203.3.1 rpki.x509.RSA.DER**

DER value of this object.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 659 of file x509.py.

10.203.3.2 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.

10.203.3.3 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.

10.203.3.4 rpki.x509.RSA.POW

Definition at line 669 of file x509.py.

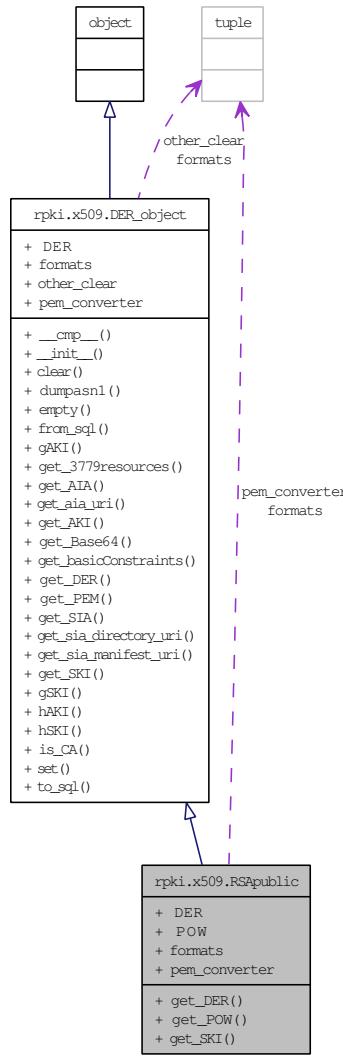
The documentation for this class was generated from the following file:

- [x509.py \(3107\)](#)

10.204 rpki.x509.RSAPublic Class Reference

Inherits [rpki::x509::DER_object](#).

Collaboration diagram for rpkix509.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.

10.204.1 Detailed Description

Class to hold an RSA public key.

Definition at line 692 of file x509.py.

10.204.2 Member Function Documentation

10.204.2.1 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.

10.204.2.2 def rpki.x509.RSAPublic.get_POW (*self*)

Get the POW value of this public key.

Definition at line 712 of file x509.py.

10.204.2.3 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.

10.204.3 Member Data Documentation**10.204.3.1 rpki.x509.RSAPublic.DER**

DER value of this object.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 708 of file x509.py.

**10.204.3.2 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.

**10.204.3.3 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.

10.204.3.4 rpki.x509.RSAPublic.POW

Definition at line 718 of file x509.py.

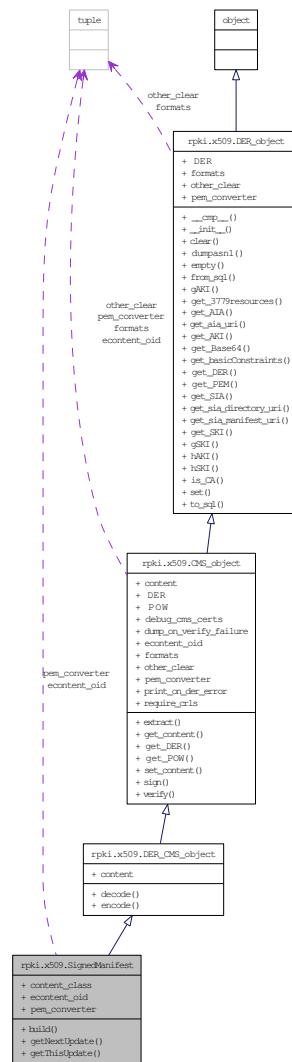
The documentation for this class was generated from the following file:

- [x509.py \(3107\)](#)

10.205 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 = rpkix.manifest.Manifest`
- tuple `econtent_oid = POWify_OID("id-ct-rpkiManifest")`
- tuple `pem_converter = PEM_converter("RPKI MANIFEST")`
PEM converter for this object.

10.205.1 Detailed Description

Class to hold a signed manifest.

Definition at line 967 of file x509.py.

10.205.2 Member Function Documentation

10.205.2.1 def rpkix509.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.

10.205.2.2 def rpkix509.SignedManifest.getNextUpdate (*self*)

Get nextUpdate value from this manifest.

Definition at line 980 of file x509.py.

10.205.2.3 def rpki.x509.SignedManifest.getThisUpdate (*self*)

Get thisUpdate value from this manifest.

Definition at line 976 of file x509.py.

10.205.3 Member Data Documentation**10.205.3.1 rpki.x509.SignedManifest.content_class = rpki.manifest.Manifest [static]**

Definition at line 973 of file x509.py.

10.205.3.2 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.

10.205.3.3 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.

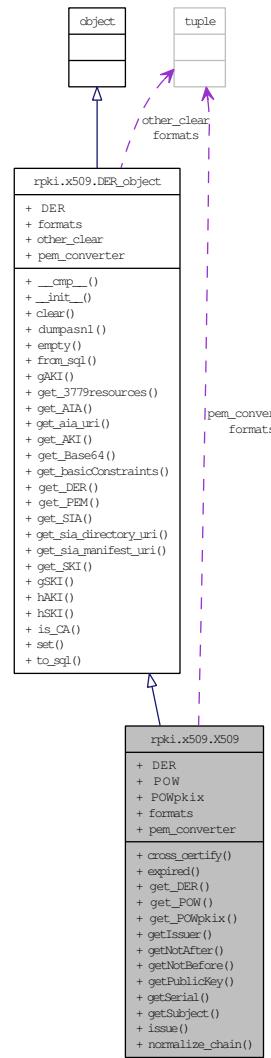
The documentation for this class was generated from the following file:

- [x509.py \(3107\)](#)

10.206 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.

10.206.1 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.

10.206.2 Member Function Documentation

10.206.2.1 def [rpkix509.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.

10.206.2.2 def rpki.x509.X509.expired (*self*)

Test whether this certificate has expired.

Definition at line 433 of file x509.py.

10.206.2.3 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.

10.206.2.4 def rpki.x509.X509.get_POW (*self*)

Get the POW value of this certificate.

Definition at line 389 of file x509.py.

10.206.2.5 def rpki.x509.X509.get_POWpkix (*self*)

Get the POW.pkix value of this certificate.

Definition at line 398 of file x509.py.

10.206.2.6 def rpki.x509.X509.getIssuer (*self*)

Get the issuer of this certificate.

Definition at line 409 of file x509.py.

10.206.2.7 def rpki.x509.X509.getNotAfter (*self*)

Get the expiration time of this certificate.

Definition at line 421 of file x509.py.

10.206.2.8 def rpki.x509.X509.getNotBefore (*self*)

Get the inception time of this certificate.

Definition at line 417 of file x509.py.

10.206.2.9 def rpki.x509.X509.getPublicKey (*self*)

Extract the public key from this certificate.

Definition at line 429 of file x509.py.

10.206.2.10 def rpki.x509.X509.getSerial (*self*)

Get the serial number of this certificate.

Definition at line 425 of file x509.py.

10.206.2.11 def rpki.x509.X509.getSubject (*self*)

Get the subject of this certificate.

Definition at line 413 of file x509.py.

10.206.2.12 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.

10.206.2.13 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.

10.206.3 Member Data Documentation**10.206.3.1 rpki.x509.X509.DER**

DER value of this object.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 382 of file x509.py.

10.206.3.2 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.

10.206.3.3 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.

10.206.3.4 rpki.x509.X509.POW

Definition at line 395 of file x509.py.

10.206.3.5 rpki.x509.X509.POWpkix

Definition at line 406 of file x509.py.

The documentation for this class was generated from the following file:

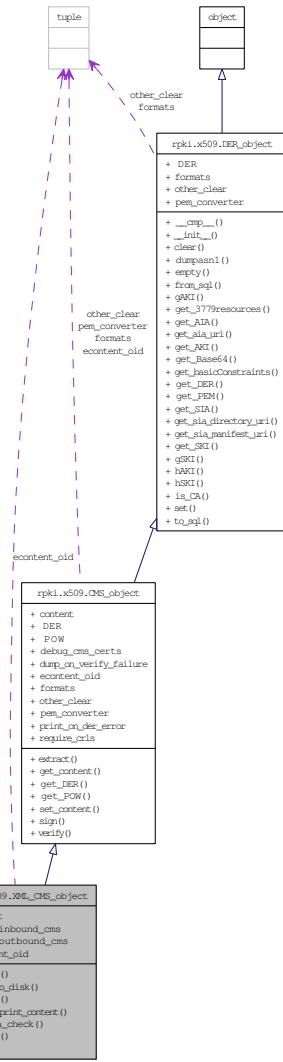
- [x509.py \(3107\)](#)

10.207 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 rpkix509.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")

10.207.1 Detailed Description

Class to hold CMS-wrapped XML protocol data.

Definition at line 1058 of file x509.py.

10.207.2 Member Function Documentation

10.207.2.1 def rpkix509.XML_CMS_object.decode (*self*, *xml*)

Decode XML and set inner content.

Definition at line 1081 of file x509.py.

10.207.2.2 def rpkix509.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.

10.207.2.3 def rpki.x509.XML_CMS_object.encode (*self*)

Encode inner content for signing.

Definition at line 1077 of file x509.py.

10.207.2.4 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.

10.207.2.5 def rpki.x509.XML_CMS_object.schema_check (*self*)

Handle XML RelaxNG schema check.

Definition at line 1089 of file x509.py.

10.207.2.6 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.

10.207.2.7 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.

10.207.3 Member Data Documentation**10.207.3.1 rpki.x509.XML_CMS_object.content**

Reimplemented from [rpki.x509.CMS_object](#).

Definition at line 1083 of file x509.py.

**10.207.3.2 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.

**10.207.3.3 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.

**10.207.3.4 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:

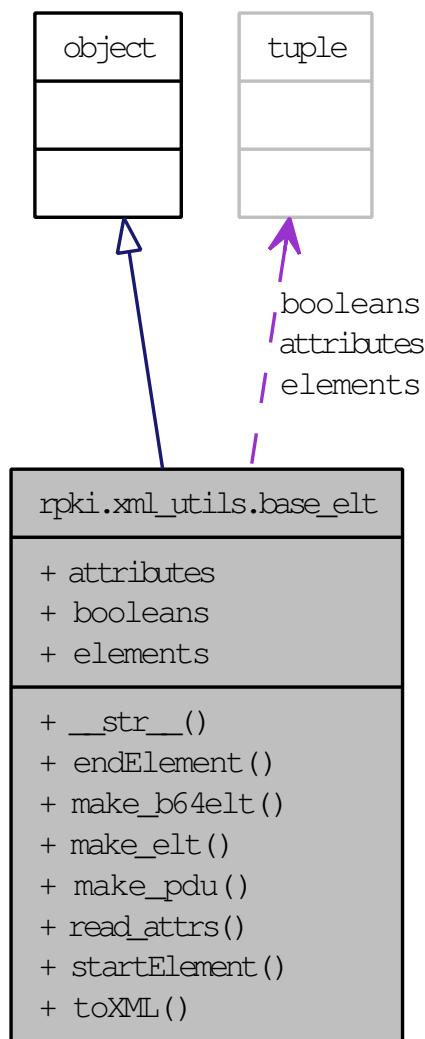
- [x509.py \(3107\)](#)

10.208 rpki.xml_utils.base_elt Class Reference

Inherits [object](#).

Inherited by [rpkি.left_right.list_received_resources_elt](#), [rpkি.left_right.list_resources_elt](#), [rpkি.left_right.list_roa_requests_elt](#), [rpkি.publication.publication_object_elt](#), [rpkি.xml_utils.data_elt](#), and [rpkি.xml_utils.text_elt](#).

Collaboration diagram for rpkি.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.

10.208.1 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`.

10.208.2 Member Function Documentation

10.208.2.1 def rpk.xml_utils.base_elt.__str__ (*self*)

Convert a `base_elt` object to string format.

Reimplemented in [rpk.publication.report_error_elt](#).

Definition at line 201 of file `xml_utils.py`.

10.208.2.2 def rpk.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`.

10.208.2.3 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`.

10.208.2.4 def rpki.xml_utils.base_elt.make_elt (*self*)

XML element constructor.

Definition at line 178 of file `xml_utils.py`.

10.208.2.5 def rpki.xml_utils.base_elt.make_pdu (*cls*, *kargs*)

Generic PDU constructor.

Definition at line 208 of file `xml_utils.py`.

10.208.2.6 def rpki.xml_utils.base_elt.readAttrs (*self*, *attrs*)

Template-driven attribute reader.

Definition at line 166 of file `xml_utils.py`.

10.208.2.7 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`.

10.208.2.8 def rpkি.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`.

10.208.3 Member Data Documentation

10.208.3.1 rpkি::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`.

10.208.3.2 rpkি::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`.

10.208.3.3 rpkি::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:

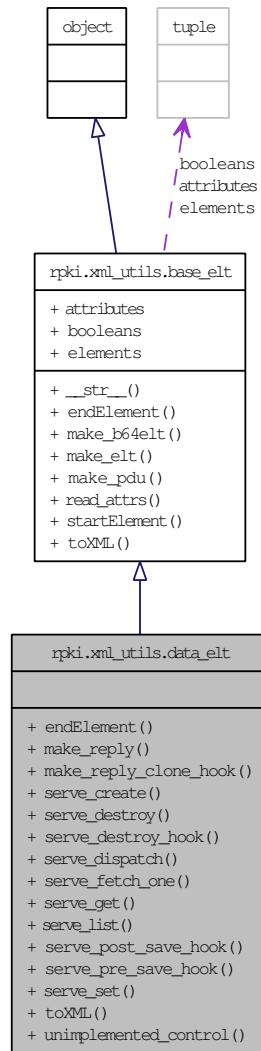
- [xml_utils.py \(2836\)](#)

10.209 rpkি.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 rpkixml_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](#)

10.209.1 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`.

10.209.2 Member Function Documentation

10.209.2.1 def rpk.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 [rpk.xml_utils.base_elt](#).

Reimplemented in [rpk.left_right.child_elt](#), and [rpk.publication.client_elt](#).

Definition at line 249 of file `xml_utils.py`.

10.209.2.2 def rpk.xml_utils.data_elt.make_reply (*self, r_pdu = None*)

Construct a reply PDU.

Definition at line 275 of file `xml_utils.py`.

10.209.2.3 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`.

10.209.2.4 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`.

10.209.2.5 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`.

10.209.2.6 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`.

10.209.2.7 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`.

10.209.2.8 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.

10.209.2.9 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.

10.209.2.10 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.

10.209.2.11 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.

10.209.2.12 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.

10.209.2.13 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`.

10.209.2.14 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`.

10.209.2.15 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:

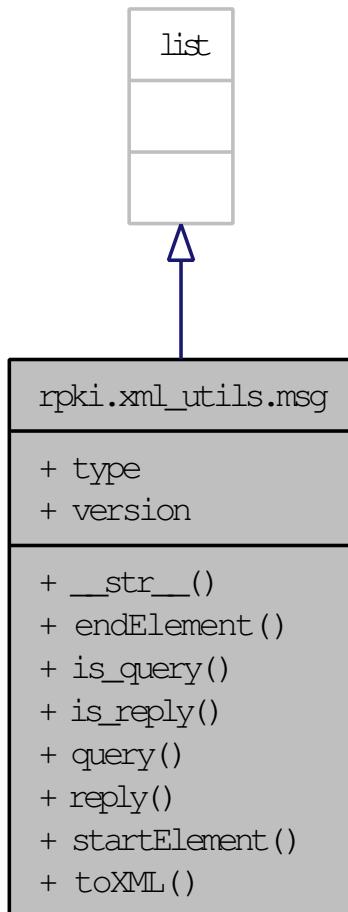
- [xml_utils.py \(2836\)](#)

10.210 rpki.xml_utils.msg Class Reference

Inherits list.

Inherited by [rpki.left_right.msg](#), and [rpki.publication.msg](#).

Collaboration diagram for rpkி.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](#)

10.210.1 Detailed Description

Generic top-level PDU.

Definition at line 416 of file xml_utils.py.

10.210.2 Member Function Documentation**10.210.2.1 def rpkixml_utils.msg.__str__ (*self*)**

Convert msg object to string.

Definition at line 442 of file xml_utils.py.

10.210.2.2 def rpkixml_utils.msg.endElement (*self, stack, name, text*)

Handle top-level PDU.

Definition at line 434 of file xml_utils.py.

10.210.2.3 def rpkixml_utils.msg.is_query (*self*)

Is this msg a query?

Definition at line 468 of file xml_utils.py.

10.210.2.4 def rpkixml_utils.msg.is_reply (*self*)

Is this msg a reply?

Definition at line 472 of file xml_utils.py.

10.210.2.5 def rpki.xml_utils.msg.query (*cls, args*)

Create a query PDU.

Definition at line 455 of file xml_utils.py.

10.210.2.6 def rpki.xml_utils.msg.reply (*cls, args*)

Create a reply PDU.

Definition at line 462 of file xml_utils.py.

10.210.2.7 def rpki.xml_utils.msg.startElement (*self, stack, name, attrs*)

Handle top-level PDU.

Definition at line 421 of file xml_utils.py.

10.210.2.8 def rpki.xml_utils.msg.toXML (*self*)

Generate top-level PDU.

Definition at line 446 of file xml_utils.py.

10.210.3 Member Data Documentation**10.210.3.1 rpki.xml_utils.msg.type**

Definition at line 427 of file xml_utils.py.

10.210.3.2 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:

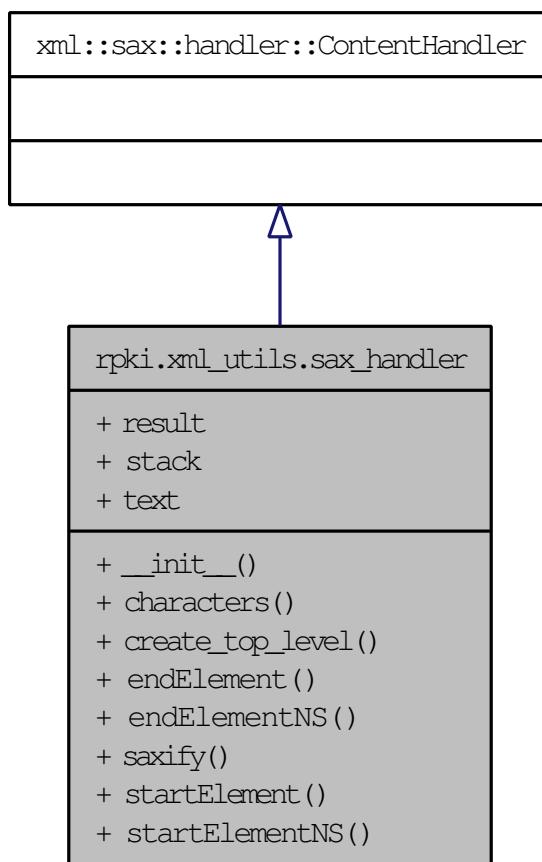
- [xml_utils.py \(2836\)](#)

10.211 rpkি.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 rpkি.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](#)

10.211.1 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`.

10.211.2 Member Function Documentation

10.211.2.1 def rpk.xml_utils.sax_handler.__init__ (*self*)

Initialize SAX handler.

Definition at line 53 of file `xml_utils.py`.

10.211.2.2 def rpkি.xml_utils.sax_handler.characters (*self*, *content*)

Accumulate a chuck of element content (text).

Definition at line 69 of file xml_utils.py.

10.211.2.3 def rpkি.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.

10.211.2.4 def rpkি.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.

10.211.2.5 def rpkি.xml_utils.sax_handler.endElementNS (*self*, *name*, *qname*)

Redirect endElementNS() events to endElement().

Definition at line 65 of file xml_utils.py.

10.211.2.6 def rpkি.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.

10.211.2.7 def rpkixml_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.

10.211.2.8 def rpkixml_utils.sax_handler.startElementNS (*self*, *name*, *qname*, *attrs*)

Redirect startElementNS() events to startElement().

Definition at line 61 of file xml_utils.py.

10.211.3 Member Data Documentation**10.211.3.1 rpkixml_utils.sax_handler.result**

Definition at line 97 of file xml_utils.py.

10.211.3.2 rpkixml_utils.sax_handler.stack

Definition at line 59 of file xml_utils.py.

10.211.3.3 rpkixml_utils.sax_handler.text

Definition at line 58 of file xml_utils.py.

The documentation for this class was generated from the following file:

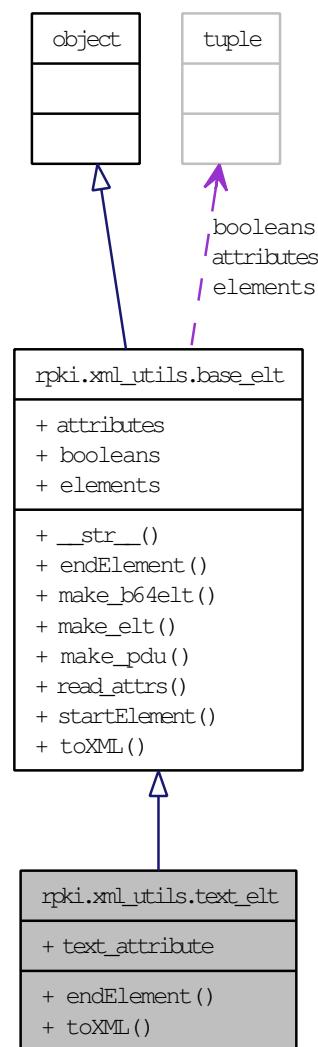
- [xml_utils.py \(2836\)](#)

10.212 rpkি.xml_utils.text_elt Class Reference

Inherits rpkি::xml_utils::base_elt.

Inherited by rpkি.left_right.list_published_objects_elt, rpkি.left_right.report_error_elt, and rpkি.publication.report_error_elt.

Collaboration diagram for rpkি.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.

10.212.1 Detailed Description

Virtual base class for XML message elements that contain text.

Definition at line 219 of file `xml_utils.py`.

10.212.2 Member Function Documentation

10.212.2.1 def rpkி.xml_utils.text_elt.endElement (*self*, *stack*, *name*, *text*)

Extract text from parsed XML.

Reimplemented from [rpkி.xml_utils.base_elt](#).

Definition at line 228 of file `xml_utils.py`.

10.212.2.2 def rpkி.xml_utils.text_elt.toXML (*self*)

Insert text into generated XML.

Reimplemented from [rpkி.xml_utils.base_elt](#).

Definition at line 235 of file `xml_utils.py`.

10.212.3 Member Data Documentation

10.212.3.1 **rpkி::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 \(2836\)](#)

10.213 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 \(2424\)](#)

10.214 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 \(2424\)](#)

10.215 TextWrapper Class Reference

Inherited by [irbe_cli.UsageWrapper](#).

The documentation for this class was generated from the following file:

- [irbe_cli.py \(3107\)](#)

10.216 ContentHandler Class Reference

Inherited by [rpki.xml_utils.sax_handler](#).

The documentation for this class was generated from the following file:

- [xml_utils.py \(2836\)](#)

11 File Documentation

11.1 __doc__.py File Reference

Packages

- package [rpki.__doc__](#)

11.2 __init__.py File Reference

Packages

- package [rpki](#)

11.3 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](#)

11.4 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

11.5 config.py File Reference

Classes

- class [rpki.config.parser](#)

Packages

- package [rpki.config](#)

11.6 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.DBConsistencyError](#)
- 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.ReceivedTLSACert](#)
- class [rpki.exceptions.RPKI_Exception](#)
- class [rpki.exceptions.ServerShuttingDown](#)
- class [rpki.exceptions.SKIMismatch](#)
- class [rpki.exceptions.SubprocessError](#)
- class [rpki.exceptions.TLSValidationrror](#)
- class [rpki.exceptions.UnexpectedCMSCerts](#)
- class [rpki.exceptions.UnexpectedCMSCRLs](#)

- class [rpki.exceptions.UnparsableCMDSER](#)
- class [rpki.exceptions.UpstreamError](#)
- class [rpki.exceptions.WrongEContentType](#)

Packages

- package [rpki.exceptions](#)

11.7 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.

- `rpkி::https.debug_tls_certs = False`
Verbose chatter about TLS certificates.
- tuple `rpkி::https.default_client_timeout = rpkி.sundial.timedelta(minutes = 15)`
Default HTTP client connection timeout.
- tuple `rpkி::https.default_http_version = (1, 0)`
Preferred HTTP version.
- tuple `rpkி::https.default_server_timeout = rpkὶ.sundial.timedelta(minutes = 20)`
Default HTTP server connection timeouts.
- string `rpkி::https.rpki_content_type = "application/x-rpki"`
HTTP content type used for all RPKI messages.
- tuple `rpkி::https.supported_address_families = (socket.AF_INET, socket.AF_INET6)`
IP address families to support.
- `rpkி::https.want_persistent_client = False`
Whether we want persistent HTTP client streams, when server also supports them.
- `rpkி::https.want_persistent_server = False`
Whether we want persistent HTTP server streams, when client also supports them.

11.8 ipaddrs.py File Reference

Classes

- class `rpkி.ipaddrs.v4addr`
- class `rpkி.ipaddrs.v6addr`

Packages

- package `rpkி.ipaddrs`

11.9 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

11.10 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.bpkı_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"))`

11.11 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

- `rpkid::left_right.enforce_strict_up_down_xml_sender` = False

11.12 log.py File Reference

Classes

- class `rpki.log.logger`

Packages

- package `rpki.log`

Functions

- def `rpkilog.init`
- def `rpkilog.set_trace`
- def `rpkilog.trace`
- def `rpkilog.traceback`

Variables

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

Whether call tracing is enabled.

- tuple `rpkilog.error` = logger(syslog.LOG_ERR)
- tuple `rpkilog.info` = logger(syslog.LOG_INFO)
- tuple `rpkilog.note` = logger(syslog.LOG_NOTICE)
- int `rpkilog.pid` = 0
- string `rpkilog.tag` = ""
- `rpkilog.use_syslog` = True

Whether to use syslog.

- tuple `rpkilog.warn` = logger(syslog.LOG_WARNING)

11.13 manifest.py File Reference

Classes

- class `rpkimani.Manifest`
- class `rpkimani.FileAndHash`
- class `rpkimani.FilesAndHashes`

Packages

- package `rpkimani`

11.14 oids.py File Reference

Packages

- package `rpkioids`

Variables

- tuple `rpkি::oids.name2oid` = dict((v, k) for k, v in oid2name.items())
Mapping table of string names to OIDs.
- dictionary `rpkি::oids.oid2name`
Mapping table of OIDs to conventional string names.

11.15 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

11.16 publication.py File Reference

Classes

- class `rpkি.publication.certificate_elt`
- class `rpkি.publication.client_elt`
- class `rpkি.publication.cms_msg`
- class `rpkি.publication.config_elt`
- class `rpkি.publication.control_elt`
- class `rpkি.publication.crl_elt`
- class `rpkি.publication.manifest_elt`
- class `rpkি.publication.msg`
- class `rpkি.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](#)

11.17 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.

11.18 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.

11.19 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](#)

11.20 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,`

11.21 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`

11.22 rpkid.py File Reference

Packages

- package [rpkid](#)

Functions

- def [rpkid.main](#)

Variables

- string [rpkid.cfg_file](#) = "rpkid.conf"
- [rpkid.profile](#) = None

11.23 sql.py File Reference

Classes

- class [rpki.sql.session](#)
- class [rpki.sql.sql_persistent](#)
- class [rpki.sql.template](#)

Packages

- package [rpki.sql](#)

11.24 sundial.py File Reference

Classes

- class [rpki.sundial.datetime](#)
- class [rpki.sundial.timedelta](#)

Packages

- package [rpki.sundial](#)

Functions

- def `rpkி::sundial._cast`
- def `rpkி::sundial.now`
- def `rpkி::sundial.test`

11.25 up_down.py File Reference

Classes

- class `rpkி.up_down.base_elt`
- class `rpkி.up_down.certificate_elt`
- class `rpkி.up_down.class_elt`
- class `rpkி.up_down.class_response_syntax`
- class `rpkி.up_down.cms_msg`
- class `rpkième.up_down.error_response_pdu`
- class `rpkième.up_down.issue_pdu`
- class `rpkième.up_down.issue_response_pdu`
- class `rpkième.up_down.list_pdu`
- class `rpkième.up_down.list_response_pdu`
- class `rpkième.up_down.message_pdu`
- class `rpkième.up_down.multi_uri`
- class `rpkième.up_down.revoke_pdu`
- class `rpkième.up_down.revoke_response_pdu`
- class `rpkième.up_down.revoke_syntax`
- class `rpkième.up_down.sax_handler`

Packages

- package `rpkième.up_down`

Variables

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

11.26 x509.py File Reference

Classes

- class `rpkième.x509.CMS_object`
- class `rpkième.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](#)

11.27 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__`
 `rpkii::sundial::timedelta`, 512
`__add__`
 `rpkii::sundial::datetime`, 505
 `rpkii::sundial::timedelta`, 512
`__call__`
 `irbe_cli::UsageWrapper`, 148
 `rpkii::async::iterator`, 168
 `rpkii::async::sync_wrapper`, 172
 `rpkii::https::caller`, 247
 `rpkii::log::logger`, 349
`__cmp__`
 `rpkii::async::timer`, 176
 `rpkii::resource_set::resource_range`,
 398
 `rpkii::resource_set::roa_prefix`, 424
 `rpkii::x509::DER_object`, 576
`__del__`
 `rpkii::async::timer`, 176
`__div__`
 `rpkii::sundial::timedelta`, 512
`__doc__.py`, 632
`__eq__`
 `rpkii::resource_set::resource_bag`,
 394
`__floordiv__`
 `rpkii::sundial::timedelta`, 512
`__init__`
 `pubd::pubd_context`, 150
 `rpkii::async::gc_summary`, 166
 `rpkii::async::iterator`, 168
 `rpkii::async::sync_wrapper`, 172
 `rpkii::async::timer`, 176
 `rpkii::cli::Cmd`, 181
 `rpkii::config::parser`, 186
 `rpkii::https::caller`, 247
 `rpkii::https::http_client`, 250
 `rpkii::https::http_listener`, 256
 `rpkii::https::http_message`, 259
 `rpkii::https::http_queue`, 263
 `rpkii::https::http_request`, 267
 `rpkii::https::http_response`, 270

`rpkii::https::http_server`, 273
`rpkii::https::http_stream`, 279
`rpkii::log::logger`, 349
`rpkii::manifest::FileAndHash`, 351
`rpkii::manifest::FilesAndHashes`, 352
`rpkii::manifest::Manifest`, 354
`rpkii::resource_set::resource_bag`,
 394
`rpkii::resource_set::resource_range`,
 398
`rpkii::resource_set::resource_set`, 410
`rpkii::resource_set::roa_prefix`, 424
`rpkii::resource_set::roa_prefix_set`,
 432
`rpkii::roa::ROAIPAddress`, 438
`rpkii::roa::ROAIPAddresses`, 440
`rpkii::roa::ROAIPAddressFamilies`,
 441
`rpkii::roa::ROAIPAddressFamily`,
 442
`rpkii::roa::RouteOriginAttestation`,
 444
`rpkii::rpki_engine::child_cert_obj`,
 463
`rpkii::rpki_engine::publication_-`
 queue, 468
`rpkii::rpki_engine::revoked_cert_obj`,
 471
`rpkii::rpki_engine::roa_obj`, 475
`rpkii::rpki_engine::rpkid_context`,
 483
`rpkii::sql::session`, 490
`rpkii::sql::template`, 502
`rpkii::up_down::class_elt`, 522
`rpkii::up_down::class_response_-`
 syntax, 526
`rpkii::up_down::error_response_pdu`,
 531
`rpkii::up_down::multi_uri`, 549
`rpkii::x509::DeadDrop`, 571
`rpkii::x509::DER_object`, 576
`rpkii::x509::PEM_converter`, 583

rpki::xml_utils::sax_handler, 626
__init__.py(3150), 632
__mul__
 rpki::sundial::timedelta, 512
__ne__
 rpki::resource_set::resource_bag,
 394
__neg__
 rpki::sundial::timedelta, 512
__new__
 rpki::ipaddrs::v4addr, 286
 rpki::ipaddrs::v6addr, 289
__pos__
 rpki::sundial::timedelta, 512
__radd__
 rpki::sundial::datetime, 505
 rpki::sundial::timedelta, 512
__rdiv__
 rpki::sundial::timedelta, 513
__repr__
 rpki::async::iterator, 169
 rpki::async::timer, 176
__rfloordiv__
 rpki::sundial::timedelta, 513
__rmul__
 rpki::sundial::timedelta, 513
__rsub__
 rpki::sundial::datetime, 505
 rpki::sundial::timedelta, 513
__str__
 rpki::https::http_message, 259
 rpki::ipaddrs::v4addr, 286
 rpki::ipaddrs::v6addr, 289
 rpki::publication::report_error_elt,
 386
 rpki::resource_set::resource_bag,
 395
rpki::resource_set::resource_range_-
 as, 400
rpki::resource_set::resource_range_-
 ip, 403
rpki::resource_set::resource_set, 410
rpki::resource_set::roa_prefix, 424
rpki::resource_set::roa_prefix_set,
 432
rpki::sundial::datetime, 506
rpki::up_down::message_pdu, 545
rpki::up_down::multi_uri, 550
rpki::xml_utils::base_elt, 613
rpki::xml_utils::msg, 623
__sub__
 rpki::sundial::datetime, 506
 rpki::sundial::timedelta, 513
_add
 rpki::rpki_engine::publication_-
 queue, 468
_bs2long
 rpki::resource_set, 86
_cast
 rpki::sundial, 91
_comm
 rpki::resource_set::resource_set, 410
_exceptions_enabled
 rpki::sql::session, 491
_find_xia_uri
 rpki::x509, 95
_long2bs
 rpki::resource_set, 86
_prefixlen
 rpki::resource_set::resource_range_-
 ip, 403
_raiseExitNow
 rpki::async, 64
_regexp
 rpki::config::parser, 188
_repl
 rpki::config::parser, 186
_rsplit
 rpki::resource_set, 86
_wrap_execute
 rpki::sql::session, 490
_yes_or_no_prompts
 rpki::cli, 67
activate
 rpki::rpki_engine::ca_detail_obj,
 448
address
 rpki::roa::ROAIPAddress, 439
addresses
 rpki::roa::ROAIPAddressFamily,
 443

addressFamily
 rpki::roa::ROAIPAddressFamily,
 443

af
 rpki::https::http_client, 253

afi
 rpki::resource_set::resource_set_-
 ipv4, 420
 rpki::resource_set::resource_set_-
 ipv6, 422

argv
 irbe_cli, 47

asID
 rpki::roa::RouteOriginAttestation,
 444

asn
 rpki::left_right::list_resources_elt,
 317
 rpki::resource_set::resource_bag,
 396
 rpki::rpki_engine::roa_obj, 478

assert_pristine
 rpki::sql::session, 490

async.py(3191), 632

asynchat::async_chat, 98

asyncore::dispatcher, 98

attributes
 rpki::left_right::bsc_elt, 293
 rpki::left_right::child_elt, 299
 rpki::left_right::list_published_-
 objects_elt, 311
 rpki::left_right::list_received_-
 resources_elt, 313
 rpki::left_right::list_resources_elt,
 317
 rpki::left_right::list_roa_requests_-
 elt, 319
 rpki::left_right::parent_elt, 327
 rpki::left_right::report_error_elt, 332
 rpki::left_right::repository_elt, 336
 rpki::left_right::self_elt, 346
 rpki::publication::client_elt, 360
 rpki::publication::config_elt, 367
 rpki::publication::publication_-
 object_elt, 383

rpki::publication::report_error_elt,
 387

rpki::xml_utils::base_elt, 615

b
 rpki::x509::PEM_converter, 584

base_uri
 rpki::publication::client_elt, 360

bits
 rpki::ipaddrs::v4addr, 287
 rpki::ipaddrs::v6addr, 289

body
 rpki::https::http_message, 261

booleans
 rpki::left_right::bsc_elt, 293
 rpki::left_right::child_elt, 299
 rpki::left_right::parent_elt, 327
 rpki::left_right::self_elt, 346
 rpki::xml_utils::base_elt, 615

bpkি_cert
 irbe_cli::cmd_elt_mixin, 111
 rpki::left_right::child_elt, 299
 rpki::left_right::repository_elt, 336
 rpki::left_right::self_elt, 346
 rpki::publication::client_elt, 361

bpkি_cms_cert
 irbe_cli::cmd_elt_mixin, 111
 rpki::left_right::parent_elt, 327

bpkি_cms_glue
 irbe_cli::cmd_elt_mixin, 111
 rpki::left_right::parent_elt, 327

bpkি_crl
 irbe_cli::config_elt, 115

bpkি_glue
 irbe_cli::cmd_elt_mixin, 111
 rpki::left_right::child_elt, 299
 rpki::left_right::repository_elt, 336
 rpki::left_right::self_elt, 346
 rpki::publication::client_elt, 361

bpkি_https_cert
 irbe_cli::cmd_elt_mixin, 111
 rpki::left_right::parent_elt, 328

bpkি_https_glue
 irbe_cli::cmd_elt_mixin, 111
 rpki::left_right::parent_elt, 328

bpkি_ta

irdbd, 51
pubd::pubd_context, 151
rootd, 59
rpki::rpki_engine::rpkid_context, 485
bsc
 rpki::left_right::data_elt, 304
bscs
 rpki::left_right::self_elt, 342
buffer
 rpki::https::http_stream, 284
build
 rpki::x509::ROA, 590
 rpki::x509::SignedManifest, 600
build_https_ta_cache
 pubd::pubd_context, 150
 rpki::https, 72
 rpki::rpki_engine::rpkid_context, 483
ca
 rpki::rpki_engine::ca_detail_obj, 448
ca_cert_uri
 rpki::rpki_engine::ca_detail_obj, 452
ca_detail
 rpki::rpki_engine::child_cert_obj, 463
 rpki::rpki_engine::revoked_cert_obj, 471
 rpki::rpki_engine::roa_obj, 475
ca_detail_id
 rpki::rpki_engine::child_cert_obj, 465
 rpki::rpki_engine::revoked_cert_obj, 472
 rpki::rpki_engine::roa_obj, 478
ca_details
 rpki::rpki_engine::ca_obj, 456
ca_from_class_name
 rpki::left_right::child_elt, 297
ca_id
 rpki::rpki_engine::ca_detail_obj, 452
cache
 rpki::sql::session, 492
cache_clear
 rpki::sql::session, 490
calculate_SKI
 rpki::x509, 95
call_pubd
 irbe_cli, 47
 rpki::left_right::repository_elt, 335
 rpki::rpki_engine::publication_queue, 468
call_rpkid
 irbe_cli, 47
callback
 rpki::https::http_request, 268
caller_function
 rpki::async::iterator, 169
cancel
 rpki::async::timer, 176
cas
 rpki::left_right::parent_elt, 325
cb
 rpki::async::sync_wrapper, 172
cert
 rpki::https::http_client, 253
 rpki::https::http_listener, 257
 rpki::https::http_queue, 264
 rpki::rpki_engine::child_cert_obj, 465
 rpki::rpki_engine::roa_obj, 478
 rpki::up_down::certificate_elt, 520
cert_url
 rpki::up_down::certificate_elt, 520
 rpki::up_down::class_elt, 523
certs
 rpki::up_down::class_elt, 523
cfg
 irbe_cli, 47
 irdbd, 51
 rootd, 59
 rpki::config::parser, 188
cfg_file
 irbe_cli, 48
 irdbd, 51
 pubd, 55
 rootd, 59
 rpkid, 97

characters
 rpki::xml_utils::sax_handler, 626

check_allowed_uri
 rpki::publication::client_elt, 359

check_for_updates
 rpki::rpki_engine::ca_obj, 456

check_response
 rpki::up_down::base_elt, 516
 rpki::up_down::error_response_pdu,
 531
 rpki::up_down::issue_response_pdu,
 539

check_valid_rpki
 rpki::x509::PKCS10, 586

checkpoint
 rpki::rpki_engine::rpkid_context,
 483

child
 rpki::rpki_engine::child_cert_obj,
 463

child_bpki_cert
 rootd, 59

child_certs
 rpki::left_right::child_elt, 297
 rpki::rpki_engine::ca_detail_obj,
 448

child_id
 rpki::rpki_engine::child_cert_obj,
 465

children
 rpki::left_right::bsc_elt, 292
 rpki::left_right::self_elt, 342

chunk_body
 rpki::https::http_stream, 279

chunk_discard_crlf
 rpki::https::http_stream, 279

chunk_discard_trailer
 rpki::https::http_stream, 279

chunk_handler
 rpki::https::http_stream, 284

chunk_header
 rpki::https::http_stream, 279

class_name
 rpki::up_down::class_elt, 523
 rpki::up_down::issue_pdu, 536
 rpki::up_down::revoke_pdu, 553

 rpki::up_down::revoke_syntax, 556

classes
 rpki::up_down::class_response_-
 syntax, 527

clear
 rpki::async::timer, 176
 rpki::x509::DER_object, 576

clear_https_ta_cache
 pubd::pubd_context, 150

rpki::left_right::child_elt, 299

rpki::publication::client_elt, 361

rpki::rpki_engine::rpkid_context,
 483

cli.py(3191), 633

client
 rpki::https, 72
 rpki::https::http_queue, 264

client_cert
 rpki::https::caller, 247

client_getopt
 irbe_cli::cmd_elt_mixin, 109

client_handler
 pubd::pubd_context, 151

client_key
 rpki::https::caller, 247

client_poll
 rpki::left_right::self_elt, 342

client_query_bpki_cert
 irbe_cli::cmd_elt_mixin, 109

client_query_bpki_cms_cert
 irbe_cli::cmd_elt_mixin, 109

client_query_bpki_crl
 irbe_cli::config_elt, 115

client_query_bpki_https_cert
 irbe_cli::cmd_elt_mixin, 110

client_query_cms_glue
 irbe_cli::cmd_elt_mixin, 110

client_query_glue
 irbe_cli::cmd_elt_mixin, 110

client_query_https_glue
 irbe_cli::cmd_elt_mixin, 110

client_query_signing_cert
 irbe_cli::bsc_elt, 100

client_query_signing_cert_crl
 irbe_cli::bsc_elt, 100

client_queues

rpkii::https, 73
client_reply_decode
 irbe_cli::bsc_elt, 100
 irbe_cli::reply_elt_mixin, 139
client_reply_show
 irbe_cli::reply_elt_mixin, 140
client_ta
 irdbd, 51
 rootd, 59
client_url_regexp
 pubd::pubd_context, 151
close
 rpkii::https::http_stream, 279
 rpkii::sql::session, 490
cmd
 rpkii::https::http_request, 268
cmd::Cmd, 98
cmdloop_with_history
 rpkii::cli::Cmd, 181, 183
cms_msg
 irbe_cli::left_right_proto, 121
 irbe_cli::publication_proto, 136
code
 rpkii::https::http_response, 270
codes
 rpkii::up_down::error_response_pdu, 532
collect_incoming_data
 rpkii::https::http_stream, 280
columns
 rpkii::sql::template, 502
complete_help
 rpkii::cli::Cmd, 181
completenames
 rpkii::cli::Cmd, 182
compose_response
 rootd, 57
config.py(3107), 633
config_id
 rpkii::publication::config_elt, 367
connect
 rpkii::sql::session, 490
construct_sia_uri
 rpkii::rpkii_engine::ca_obj, 457
contains
 rpkii::resource_set::resource_set, 411
content
 rpkii::x509::CMS_object, 563
 rpkii::x509::DER_CMS_object, 573
 rpkii::x509::XML_CMS_object, 611
content_class
 rpkii::x509::ROA, 590
 rpkii::x509::SignedManifest, 601
control_handler
 pubd::pubd_context, 151
convert_to_seconds
 rpkii::sundial::timedelta, 513
create
 rpkii::rpkii_engine::ca_detail_obj, 448
 rpkii::rpkii_engine::ca_obj, 457
 rpkii::x509::PKCS10, 586
create_ca
 rpkii::x509::PKCS10, 586
create_top_level
 rpkii::xml_utils::sax_handler, 627
crl_interval
 rpkii::left_right::self_elt, 347
crl_published
 rpkii::rpkii_engine::ca_detail_obj, 452
crl_published_callback
 rpkii::rpkii_engine::ca_detail_obj, 448
crl_uri
 rpkii::rpkii_engine::ca_detail_obj, 448
crl_uri_tail
 rpkii::rpkii_engine::ca_detail_obj, 449
cron
 rpkii::left_right::self_elt, 342
 rpkii::rpkii_engine::rpkid_context, 483
cron_keepalive
 rpkii::rpkii_engine::rpkid_context, 485
cron_period
 rpkii::rpkii_engine::rpkid_context, 485
cron_timeout

rpki::rpki_engine::rpkid_context,
 485
cron_timer
 rpki::rpki_engine::rpkid_context,
 485
cronjob_handler
 rpki::rpki_engine::rpkid_context,
 483
cross_certify
 rpki::x509::X509, 603
cur
 irdbd, 51
 rpki::sql::session, 492
database
 rpki::sql::session, 492
datum_type
 rpki::resource_set::resource_range_-
 as, 400
 rpki::resource_set::resource_range_-
 ipv4, 406
 rpki::resource_set::resource_range_-
 ipv6, 408
db
 irdbd, 51
 rpki::sql::session, 492
debug
 rpki::https::caller, 248
 rpki::log, 79
debug_cms_certs
 rpki::x509::CMS_object, 563
debug_http
 rpki::https, 73
debug_tls_certs
 rpki::https, 73
decode
 rpki::x509::DER_CMS_object, 573
 rpki::x509::XML_CMS_object, 609
default_client_timeout
 rpki::https, 73
default_http_version
 rpki::https, 73
default_pubd_handler
 rpki::left_right::repository_elt, 335
default_section
 rpki::config::parser, 189
default_server_timeout
 rpki::https, 73
defer
 rpki::async, 64
deferred_queue
 rpki::async, 65
del_subject_cert
 rootd, 57
del_subject_pkcs10
 rootd, 57
delete
 rpki::rpki_engine::ca_detail_obj,
 449
 rpki::rpki_engine::ca_obj, 457
 rpki::sql::template, 502
DER
 rpki::x509::CMS_object, 564
 rpki::x509::CRL, 569
 rpki::x509::DER_object, 581
 rpki::x509::PKCS10, 587
 rpki::x509::RSA, 594
 rpki::x509::RSAPublic, 598
 rpki::x509::X509, 606
description
 rpki::up_down::error_response_pdu,
 532
detach
 rpki::https::http_queue, 263
difference
 rpki::resource_set::resource_set, 411
dirty
 rpki::sql::session, 492
do_EOF
 rpki::cli::Cmd, 182
do_exit
 rpki::cli::Cmd, 182
do_quit
 rpki::cli::Cmd, 183
doit
 rpki::async::iterator, 169
done_callback
 rpki::async::iterator, 169
dump
 rpki::x509::DeadDrop, 571
dump_inbound_cms
 rpki::x509::XML_CMS_object, 611

dump_on_verify_failure
 rpki::x509::CMS_object, 564

dump_outbound_cms
 rpki::x509::XML_CMS_object, 611

dump_to_disk
 rpki::x509::XML_CMS_object, 609

dumpasn1
 rpki::x509::DER_object, 576

dynamic_ta
 rpki::https::http_listener, 257

e
 rpki::x509::PEM_converter, 584

earlier
 rpki::sundial::datetime, 506

eb
 rpki::async::sync_wrapper, 172

econtent_oid
 rpki::x509::CMS_object, 564
 rpki::x509::ROA, 590
 rpki::x509::SignedManifest, 601
 rpki::x509::XML_CMS_object, 611

element_name
 rpki::left_right::bsc_elt, 294
 rpki::left_right::child_elt, 299
 rpki::left_right::list_published_-
 objects_elt, 311
 rpki::left_right::list_received_-
 resources_elt, 313
 rpki::left_right::list_resources_elt,
 317
 rpki::left_right::list_roa_requests_-
 elt, 319
 rpki::left_right::parent_elt, 328
 rpki::left_right::report_error_elt, 332
 rpki::left_right::repository_elt, 336
 rpki::left_right::self_elt, 347
 rpki::publication::certificate_elt, 357
 rpki::publication::client_elt, 361
 rpki::publication::config_elt, 368
 rpki::publication::crl_elt, 373
 rpki::publication::manifest_elt, 375
 rpki::publication::report_error_elt,
 387
 rpki::publication::roa_elt, 390

elements

empty
 rpki::resource_set::resource_bag,
 395
 rpki::x509::DER_object, 576

emptyline
 rpki::cli::Cmd, 182

emptyline_repeats_last_command
 rpki::cli::Cmd, 183

enable_trace
 rpki::log, 79

encode
 rpki::x509::DER_CMS_object, 573
 rpki::x509::XML_CMS_object, 609

encoding
 rpki::left_right::cms_msg, 302
 rpki::publication::cms_msg, 364
 rpki::up_down::cms_msg, 529

endElement
 rpki::left_right::child_elt, 298
 rpki::publication::client_elt, 359
 rpki::publication::publication_-
 object_elt, 381
 rpki::up_down::base_elt, 516
 rpki::up_down::certificate_elt, 519
 rpki::up_down::class_elt, 522
 rpki::up_down::error_response_pdu,
 531
 rpki::up_down::issue_pdu, 535
 rpki::xml_utils::base_elt, 613
 rpki::xml_utils::data_elt, 618
 rpki::xml_utils::msg, 623
 rpki::xml_utils::sax_handler, 627
 rpki::xml_utils::text_elt, 630

endElementNS
 rpki::xml_utils::sax_handler, 627

enforce_strict_up_down_xml_sender
 rpki::left_right, 77

EOF_exits_command_loop

rpki::cli::Cmd, 184
err
 rpki::async::sync_wrapper, 173
errback
 rpki::async::timer, 176, 178
 rpki::https::http_request, 268
error
 rpki::log, 79
error_code
 rpki::left_right::report_error_elt, 332
 rpki::publication::report_error_elt,
 387
error_text
 rpki::left_right::report_error_elt, 332
 rpki::publication::report_error_elt,
 387
event_loop
 rpki::async, 65
Exception, 98
exceptions
 rpki::up_down::error_response_pdu,
 532
exceptions.py(2907), 633
excludes
 irbe_cli::bsc_elt, 101
 irbe_cli::cmd_elt_mixin, 111
 irbe_cli::list_published_objects_elt,
 125
 irbe_cli::list_received_resources_elt,
 127
execute
 rpki::sql::session, 490
executemany
 rpki::sql::session, 491
exit_event_loop
 rpki::async, 65
ExitNow
 rpki::async, 65
expect_close
 rpki::https::http_client, 253
 rpki::https::http_server, 275
expired
 rpki::x509::X509, 604
expires
 rpki::rpk_engine::revoked_cert_obj,
 472
explicitVersion
 rpki::manifest::Manifest, 354
 rpki::roa::RouteOriginAttestation,
 444
extract
 rpki::x509::CMS_object, 562
fetch
 rpki::publication::config_elt, 366
 rpki::rpk_engine::child_cert_obj,
 464
fetch_active
 rpki::rpk_engine::ca_obj, 457
fetch_deprecated
 rpki::rpk_engine::ca_obj, 458
fetch_issue_response_candidates
 rpki::rpk_engine::ca_obj, 458
fetch_pending
 rpki::rpk_engine::ca_obj, 458
fetch_revoked
 rpki::rpk_engine::ca_obj, 458
fetchall
 rpki::sql::session, 491
file
 rpki::manifest::FileAndHash, 351
fileHashAlg
 rpki::manifest::Manifest, 354
fileList
 rpki::manifest::Manifest, 354
filename
 rpki::config::parser, 189
filename_complete
 rpki::cli::Cmd, 182
find_handler
 rpki::https::http_server, 273
format
 rpki::https::http_message, 259
format_first_line
 rpki::https::http_request, 267
 rpki::https::http_response, 270
formats
 rpki::x509::CMS_object, 564
 rpki::x509::CRL, 569
 rpki::x509::DER_object, 581
 rpki::x509::PKCS10, 587
 rpki::x509::RSA, 594

rpkii::x509::RSAPublic, 598
rpkii::x509::X509, 606

found_terminator
 rpkii::https::http_stream, 280

from_bytes
 rpkii::ipaddrs::v4addr, 286
 rpkii::ipaddrs::v6addr, 289

from_exception
 rpkii::left_right::report_error_elt, 331
 rpkii::publication::report_error_elt,
 386

from_resource_bag
 rpkii::up_down::class_elt, 522

from_rfc3779_tuples
 rpkii::resource_set::resource_bag,
 395

from_sql
 rpkii::resource_set::resource_set, 411
 rpkii::resource_set::roa_prefix_set,
 432
 rpkii::sundial::datetime, 506
 rpkii::x509::DER_object, 577

fromASN1tuple
 rpkii::sundial::datetime, 506

fromdatetime
 rpkii::sundial::datetime, 506

fromGeneralizedTime
 rpkii::sundial::datetime, 507

fromtimedelta
 rpkii::sundial::timedelta, 513

fromUTCTime
 rpkii::sundial::datetime, 507

fromXMLtime
 rpkii::sundial::datetime, 507

func
 rpkii::async::sync_wrapper, 173

gAKI
 rpkii::x509::DER_object, 577

gc_debug
 rpkii::async::timer, 178

gctx
 rpkii::rpki_engine::ca_detail_obj,
 452
 rpkii::rpki_engine::ca_obj, 460

rpkii::rpki_engine::child_cert_obj,
 465

rpkii::rpki_engine::revoked_cert_obj,
 472

rpkii::rpki_engine::roa_obj, 479

rpkii::sql::sql_persistent, 499

generate
 rpkii::rpki_engine::roa_obj, 476
 rpkii::x509::CRL, 567
 rpkii::x509::RSA, 593

generate_crl
 rpkii::rpki_engine::ca_detail_obj,
 449

generate_manifest
 rpkii::rpki_engine::ca_detail_obj,
 449

generate_manifest_cert
 rpkii::rpki_engine::ca_detail_obj,
 449

get
 rpkii::config::parser, 187

get_3779resources
 rpkii::x509::DER_object, 577

get_AIA
 rpkii::x509::DER_object, 577

get_aia_uri
 rpkii::x509::DER_object, 577

get_AKI
 rpkii::x509::DER_object, 578

get_Base64
 rpkii::x509::DER_object, 578

get_basicConstraints
 rpkii::x509::DER_object, 578

get_buffer
 rpkii::https::http_stream, 280

get_content
 rpkii::x509::CMS_object, 562

get_DER
 rpkii::x509::CMS_object, 562
 rpkii::x509::CRL, 567
 rpkii::x509::DER_object, 578
 rpkii::x509::PKCS10, 587
 rpkii::x509::RSA, 593
 rpkii::x509::RSAPublic, 597
 rpkii::x509::X509, 604

get_PEM

rpkii::x509::DER_object, 578
get_POW
 rpkii::x509::CMS_object, 562
 rpkii::x509::CRL, 568
 rpkii::x509::RSA, 593
 rpkii::x509::RSApublic, 597
 rpkii::x509::X509, 604
get_POWpkix
 rpkii::x509::CRL, 568
 rpkii::x509::PKCS10, 587
 rpkii::x509::X509, 604
get_public_DER
 rpkii::x509::RSA, 594
get_root_cert
 rootd, 57
get_RSApublic
 rpkii::x509::RSA, 594
get_SIA
 rpkii::x509::DER_object, 579
get_sia_directory_uri
 rpkii::x509::DER_object, 579
get_sia_manifest_uri
 rpkii::x509::DER_object, 579
get_SKI
 rpkii::up_down::revoke_pdu, 552
 rpkii::x509::DER_object, 579
 rpkii::x509::RSA, 594
 rpkii::x509::RSApublic, 597
get_subject_cert
 rootd, 58
get_subject_pkcs10
 rootd, 58
getboolean
 rpkii::config::parser, 187
getint
 rpkii::config::parser, 187
getIssuer
 rpkii::x509::CRL, 568
 rpkii::x509::X509, 604
getlong
 rpkii::config::parser, 187
getNextUpdate
 rpkii::x509::CRL, 568
 rpkii::x509::SignedManifest, 600
getNotAfter
 rpkii::x509::X509, 604
getNotBefore
 rpkii::x509::X509, 605
getPublicKey
 rpkii::x509::PKCS10, 587
 rpkii::x509::X509, 605
getSerial
 rpkii::x509::X509, 605
getSubject
 rpkii::x509::X509, 605
getThisUpdate
 rpkii::x509::CRL, 568
 rpkii::x509::SignedManifest, 600
gSKI
 rpkii::x509::DER_object, 579
hAKI
 rpkii::x509::DER_object, 580
handle_accept
 rpkii::https::http_listener, 256
handle_body
 rpkii::https::http_stream, 280
handle_close
 rpkii::https::http_client, 250
 rpkii::https::http_stream, 281
handle_connect
 rpkii::https::http_client, 251
handle_dispatch
 irdbd, 52
handle_error
 rpkii::https::http_client, 251
 rpkii::https::http_listener, 256
 rpkii::https::http_stream, 281
handle_list_resources
 irdbd, 50
handle_list_roa_requests
 irdbd, 50
handle_message
 rpkii::https::http_client, 251
 rpkii::https::http_server, 273
handle_no_content_length
 rpkii::https::http_client, 251
 rpkii::https::http_server, 274
handle_read
 rpkii::https::http_stream, 281
handle_timeout
 rpkii::https::http_client, 252

rpkii::https::http_stream, 281
handle_write
 rpkii::https::http_stream, 282
handler
 irdbd, 51
 rpkii::async::gc_summary, 166
 rpkii::async::timer, 177, 179
 handler_common
 pubd::pubd_context, 151
handlers
 irdbd, 52
 rootd, 59
 rpkii::https::http_listener, 257
 rpkii::https::http_server, 275
 rpkii::rpki_engine::publication_queue, 469
handles
 rpkii::left_right::bsc_elt, 294
 rpkii::left_right::child_elt, 300
 rpkii::left_right::data_elt, 306
 rpkii::left_right::parent_elt, 328
 rpkii::left_right::repository_elt, 337
 rpkii::left_right::self_elt, 347
has_option
 rpkii::config::parser, 187
has_section
 rpkii::config::parser, 188
hash
 rpkii::manifest::FileAndHash, 351
have_readline
 rpkii::cli, 67
headers
 rpkii::https::http_message, 261
help_help
 rpkii::cli::Cmd, 183
histfile
 rpkii::cli::Cmd, 184
host
 irdbd, 52
 rootd, 59
hostport
 rpkii::https::http_client, 253
 rpkii::https::http_queue, 265
hSKI
 rpkii::x509::DER_object, 580
https.py(3191), 635

https_server_host
 pubd::pubd_context, 152
 rootd, 60
 rpkii::rpki_engine::rpkid_context, 486
https_server_port
 pubd::pubd_context, 152
 rootd, 60
 rpkii::rpki_engine::rpkid_context, 486
https_ta_cache
 pubd::pubd_context, 152
 rpkii::rpki_engine::rpkid_context, 486

identchars
 rpkii::cli::Cmd, 184
index
 rpkii::sql::template, 502
info
 rpkii::log, 79
inherit
 rpkii::resource_set::resource_set, 412
 rpkii::resource_set::resource_set_as, 415
 rpkii::resource_set::resource_set_ip, 418
inherit_token
 rpkii::resource_set, 87
init
 rpkii::log, 78
initial_delay
 rpkii::rpki_engine::rpkid_context, 486
initiate_send
 rpkii::https::http_stream, 282
insert
 rpkii::sql::template, 502
intersection
 rpkii::resource_set::resource_bag, 395
 rpkii::resource_set::resource_set, 411
interval
 rpkii::async::gc_summary, 166
ipAddrBlocks

rpki::roa::RouteOriginAttestation, 444
ipaddrs.py(2424), 636
ipv4
 rpki::left_right::list_resources_elt, 317
 rpki::left_right::list_roa_requests_elt, 320
 rpki::rpki_engine::roa_obj, 479
ipv6
 rpki::left_right::list_resources_elt, 317
 rpki::left_right::list_roa_requests_elt, 320
 rpki::rpki_engine::roa_obj, 479
irbe_cert
 pubd::pubd_context, 152
 rpki::rpki_engine::rpkid_context, 486
irbe_cli, 45
 argv, 47
 call_pubd, 47
 call_rpkid, 47
 cfg, 47
 cfg_file, 48
 pem_out, 48
 q_msg, 48
 q_msg_left_right, 48
 q_msg_publication, 48
 q_pdu, 48
 top_opts, 48
 usage, 47
 usage_fill, 49
 verbose, 49
irbe_cli.py(3107), 637
irbe_cli::bsc_elt, 98
 client_query_signing_cert, 100
 client_query_signing_cert_crl, 100
 client_reply_decode, 100
 excludes, 101
 signing_cert, 101
 signing_cert_crl, 101
irbe_cli::certificate_elt, 101
irbe_cli::child_elt, 103
irbe_cli::client_elt, 105
irbe_cli::cmd_elt_mixin, 107
bpki_cert, 111
bpki_cms_cert, 111
bpki_cms_glue, 111
bpki_glue, 111
bpki_https_cert, 111
bpki_https_glue, 111
client_getopt, 109
client_query_bpki_cert, 109
client_query_bpki_cms_cert, 109
client_query_bpki_https_cert, 110
client_query_cms_glue, 110
client_query_glue, 110
client_query_https_glue, 110
excludes, 111
is_cmd, 112
usage, 110
irbe_cli::cmd_msg_mixin, 112
 usage, 113
irbe_cli::config_elt, 113
 bpki_crl, 115
 client_query_bpki_crl, 115
irbe_cli::crl_elt, 115
irbe_cli::left_right_cms_msg, 117
 saxify, 118
irbe_cli::left_right_msg, 118
 pdus, 120
irbe_cli::left_right_proto, 120
 cms_msg, 121
 msg, 121
irbe_cli::left_right_sax_handler, 122
 pdu, 123
irbe_cli::list_published_objects_elt, 123
 excludes, 125
irbe_cli::list_received_resources_elt, 125
 excludes, 127
irbe_cli::manifest_elt, 127
irbe_cli::parent_elt, 129
irbe_cli::publication_cms_msg, 131
 saxify, 133
irbe_cli::publication_msg, 133
 pdus, 135
irbe_cli::publication_proto, 135
 cms_msg, 136
 msg, 136
irbe_cli::publication_sax_handler, 137
 pdu, 138

irbe_cli::reply_elt_mixin, 138
client_reply_decode, 139
client_reply_show, 140
is_cmd, 140
irbe_cli::report_error_elt, 140
irbe_cli::repository_elt, 141
irbe_cli::roa_elt, 143
irbe_cli::self_elt, 145
irbe_cli::UsageWrapper, 147
 __call__, 148
irdb_cert
 rpki::rpki_engine::rpkid_context,
 486
irdb_query
 rpki::rpki_engine::rpkid_context,
 484
irdb_query_child_resources
 rpki::rpki_engine::rpkid_context,
 484
irdb_query_roa_requests
 rpki::rpki_engine::rpkid_context,
 484
irdb_url
 rpki::rpki_engine::rpkid_context,
 486
irdbd, 49
 bpki_ta, 51
 cfg, 51
 cfg_file, 51
 client_ta, 51
 cur, 51
 db, 51
 handle_dispatch, 52
 handle_list_resources, 50
 handle_list_roa_requests, 50
 handler, 51
 handlers, 52
 host, 52
 irdbd_cert, 52
 irdbd_key, 52
 port, 52
 rpkid_cert, 53
 server_cert, 53
 startup_msg, 53
 u, 53
irdbd.py(2913), 638
irdbd_cert
 irdbd, 52
irdbd_key
 irdbd, 52
is_CA
 rpki::x509::DER_object, 580
is_cmd
 irbe_cli::cmd_elt_mixin, 112
 irbe_cli::reply_elt_mixin, 140
is_query
 rpki::xml_utils::msg, 623
is_reply
 rpki::xml_utils::msg, 623
is_set
 rpki::async::timer, 177
issubset
 rpki::resource_set::resource_set, 411
issue
 rpki::rpki_engine::ca_detail_obj,
 450
 rpki::x509::X509, 605
issue_ee
 rpki::rpki_engine::ca_detail_obj,
 450
issue_subject_cert_maybe
 rootd, 58
issuer
 rpki::up_down::class_elt, 524
issuperset
 rpki::resource_set::resource_set, 412
item_callback
 rpki::async::iterator, 169
iterator
 rpki::async::iterator, 169
key
 rpki::https::http_client, 253
 rpki::https::http_listener, 257
 rpki::https::http_queue, 265
last_crl_sn
 rpki::rpki_engine::ca_obj, 460
last_issued_sn
 rpki::rpki_engine::ca_obj, 460
last_manifest_sn
 rpki::rpki_engine::ca_obj, 460

lastrowid
 rpki::sql::session, 491

later
 rpki::sundial::datetime, 507

latest_ca_cert
 rpki::rpki_engine::ca_detail_obj,
 452

latest_crl
 rpki::rpki_engine::ca_detail_obj,
 452

latest_manifest
 rpki::rpki_engine::ca_detail_obj,
 453

latest_manifest_cert
 rpki::rpki_engine::ca_detail_obj,
 453

left_right
 rpki::relaxng, 84

left_right.py(3191), 639

left_right_handler
 rpki::rpki_engine::rpkid_context,
 484

log
 rpki::https::http_listener, 257
 rpki::https::http_queue, 265
 rpki::https::http_stream, 284

log.py(3107), 639

log_cert
 rpki::https::http_stream, 282

log_method
 rpki::https, 72

log_query
 root::message_pdu, 161
 rpki::up_down::message_pdu, 545

long, 148

looks_like_PEM
 rpki::x509::PEM_converter, 583

maildir
 rpki::x509::DeadDrop, 571

main
 pubd, 54
 rpkid, 97

make_b64elt
 rpki::up_down::base_elt, 516
 rpki::xml_utils::base_elt, 614

make_elt
 rpki::up_down::base_elt, 516
 rpki::xml_utils::base_elt, 614

make_pdu
 rpki::xml_utils::base_elt, 614

make_prefix
 rpki::resource_set::resource_range_-
 ip, 403

make_publish
 rpki::publication::publication_-
 object_elt, 381

make_query
 rpki::up_down::message_pdu, 545

make_reply
 rpki::left_right::list_published_-
 objects_elt, 310
 rpki::left_right::list_received_-
 resources_elt, 313
 rpki::xml_utils::data_elt, 618

make_reply_clone_hook
 rpki::left_right::data_elt, 304
 rpki::xml_utils::data_elt, 618

make_withdraw
 rpki::publication::publication_-
 object_elt, 382

manifest.py(2424), 640

manifest_private_key_id
 rpki::rpki_engine::ca_detail_obj,
 453

manifest_public_key
 rpki::rpki_engine::ca_detail_obj,
 453

manifest_published
 rpki::rpki_engine::ca_detail_obj,
 453

manifest_published_callback
 rpki::rpki_engine::ca_detail_obj,
 450

manifest_uri
 rpki::rpki_engine::ca_detail_obj,
 450

manifestNumber
 rpki::manifest::Manifest, 354

map
 rpki::sql::template, 503

max

rpki::resource_set::resource_range, 398
rpki::resource_set::roa_prefix, 424
max_prefixlen
 rpki::resource_set::roa_prefix, 425
maxLength
 rpki::roa::ROAIPAddress, 439
min
 rpki::resource_set::resource_range, 398
 rpki::resource_set::resource_range_as, 401
 rpki::resource_set::roa_prefix, 425
msg
 irbe_cli::left_right_proto, 121
 irbe_cli::publication_proto, 136
 rpki::https::http_stream, 284
msgs
 rpki::rpki_engine::publication_queue, 469
multiget
 rpki::config::parser, 188
name
 rpki::left_right::sax_handler, 339
 rpki::publication::sax_handler, 392
 rpki::up_down::sax_handler, 559
name2oid
 rpki::oids, 82
name2type
 root::message_pdu, 161
 rpki::up_down::message_pdu, 547
next_crl_number
 rpki::rpki_engine::ca_obj, 458
next_manifest_number
 rpki::rpki_engine::ca_obj, 459
next_serial_number
 rpki::rpki_engine::ca_obj, 459
nextUpdate
 rpki::manifest::Manifest, 354
 rpki::rpki_engine::ca_detail_obj, 453
normalize_chain
 rpki::x509::X509, 606
normalize_headers
 rpki::https::http_message, 260
note
 rpki::log, 80
now
 rpki::sundial, 91
nsmap
 rpki::left_right::left_right_namespace, 307
 rpki::publication::publication_namespace, 379
 rpki::up_down, 93
obj
 rpki::left_right::list_published_objects_elt, 311
object, 148
oid2name
 rpki::oids, 82
oids.py(2424), 640
onecmd
 rpki::cli::Cmd, 183
other_clear
 rpki::x509::CMS_object, 564
 rpki::x509::DER_object, 581
oversized
 rpki::resource_set::resource_bag, 395
parent
 rpki::rpki_engine::ca_obj, 459
parent_id
 rpki::rpki_engine::ca_obj, 460
parent_resource_class
 rpki::rpki_engine::ca_obj, 460
parents
 rpki::left_right::bsc_elt, 292
 rpki::left_right::child_elt, 298
 rpki::left_right::repository_elt, 336
 rpki::left_right::self_elt, 342
parse
 rpki::sundial::timedelta, 514
parse_first_line
 rpki::https::http_request, 267
 rpki::https::http_response, 270
parse_from_wire
 rpki::https::http_message, 260
parse_rfc3779_tuple

rpkii::resource_set::resource_set_as,
 414
rpkii::resource_set::resource_set_ip,
 417
parse_str
 rpkii::resource_set::resource_set_as,
 414
 rpkii::resource_set::resource_set_ip,
 417
 rpkii::resource_set::roa_prefix_set,
 432
parse_type
 rpkii::https::http_client, 253
 rpkii::https::http_server, 275
parse_version
 rpkii::https::http_message, 260
password
 rpkii::sql::session, 492
path
 rpkii::https::http_request, 268
payload
 rpkii::publication::publication_-
 object_elt, 383
 rpkii::up_down::message_pdu, 547
payload_type
 rpkii::publication::certificate_elt, 357
 rpkii::publication::crl_elt, 373
 rpkii::publication::manifest_elt, 375
 rpkii::publication::publication_-
 object_elt, 383
 rpkii::publication::roa_elt, 390
pdu
 irbe_cli::left_right_sax_handler, 123
 irbe_cli::publication_sax_handler,
 138
 rootd::sax_handler, 165
 rpkii::left_right::sax_handler, 339
 rpkii::publication::sax_handler, 392
 rpkii::up_down::sax_handler, 559
pdus
 irbe_cli::left_right_msg, 120
 irbe_cli::publication_msg, 135
 rpkii::left_right::msg, 322
 rpkii::publication::msg, 377
pem_converter
 rpkii::x509::CMS_object, 565
rpkii::x509::CRL, 569
rpkii::x509::DER_object, 581
rpkii::x509::PKCS10, 588
rpkii::x509::ROA, 590
rpkii::x509::RSA, 595
rpkii::x509::RSAPublic, 598
rpkii::x509::SignedManifest, 601
rpkii::x509::X509, 606
pem_out
 irbe_cli, 48
persistent
 rpkii::https::http_message, 260
pid
 rpkii::log, 80
 rpkii::x509::DeadDrop, 571
ping
 rpkii::sql::session, 491
pkcs10
 rpkii::up_down::issue_pdu, 536
pkcs10_request
 rpkii::left_right::bsc_elt, 294
PKIX_threshhold
 rpkii::sundial::datetime, 509
port
 irdbd, 52
 rootd, 60
POW
 rpkii::x509::CMS_object, 565
 rpkii::x509::CRL, 569
 rpkii::x509::RSA, 595
 rpkii::x509::RSAPublic, 598
 rpkii::x509::X509, 607
POWify_OID
 rpkii::x509, 95
POWpkix
 rpkii::x509::CRL, 569
 rpkii::x509::PKCS10, 588
 rpkii::x509::X509, 607
prefix
 rpkii::resource_set::roa_prefix, 425
prefix_type
 rpkii::resource_set::roa_prefix_set_-
 ipv4, 435
 rpkii::resource_set::roa_prefix_set_-
 ipv6, 437
prefixlen

rpkii::resource_set::roa_prefix, 426
pretty_print_content
 rpki::x509::XML_CMS_object, 610
print_on_der_error
 rpki::x509::CMS_object, 565
priority
 rpki::log::logger, 349
private_key_id
 rpki::left_right::bsc_elt, 294
 rpki::rpki_engine::ca_detail_obj,
 453
profile
 pubd, 55
 rpkid, 97
proto
 rpki::https::caller, 248
pubd, 53
 cfg_file, 55
 main, 54
 profile, 55
pubd.py(3107), 641
pubd::pubd_context, 148
 __init__, 150
 bpki_ta, 151
 build_https_ta_cache, 150
 clear_https_ta_cache, 150
 client_handler, 151
 client_url_regexp, 151
 control_handler, 151
 handler_common, 151
 https_server_host, 152
 https_server_port, 152
 https_ta_cache, 152
 irbe_cert, 152
 pubd_cert, 152
 pubd_key, 152
 publication_base, 152
 publication_multimodule, 153
 sql, 153
pubd_cert
 pubd::pubd_context, 152
pubd_key
 pubd::pubd_context, 152
public_key
 rpki::rpki_engine::ca_detail_obj,
 454
publication
 rpki::relaxng, 84
publication.py(3107), 641
publication_base
 pubd::pubd_context, 152
publication_kludge_base
 rpki::rpki_engine::rpkid_context,
 487
publication_multimodule
 pubd::pubd_context, 153
publish
 rpki::rpki_engine::publication_ -
 queue, 468
published
 rpki::rpki_engine::child_cert_obj,
 465
 rpki::rpki_engine::roa_obj, 479
published_callback
 rpki::rpki_engine::child_cert_obj,
 464
 rpki::rpki_engine::roa_obj, 476
pydatetime::datetime, 153
pydatetime::timedelta, 153
q_msg
 irbe_cli, 48
q_msg_left_right
 irbe_cli, 48
q_msg_publication
 irbe_cli, 48
q_pdu
 irbe_cli, 48
query
 rpki::up_down::issue_pdu, 535
 rpki::up_down::list_pdu, 541
 rpki::up_down::revoke_pdu, 552
 rpki::xml_utils::msg, 623
query_up_down
 rpki::left_right::parent_elt, 325
queue
 rpki::async::timer, 179
 rpki::https::http_client, 254
 rpki::https::http_queue, 265
raise_if_error

rpki::publication::publication_object_elt, 382
rpki::publication::report_error_elt, 387
range_type
 rpki::resource_set::resource_set_as, 415
 rpki::resource_set::resource_set_ipv4, 420
 rpki::resource_set::resource_set_ipv6, 422
 rpki::resource_set::roa_prefix_ipv4, 428
 rpki::resource_set::roa_prefix_ipv6, 430
readAttrs
 rpki::xml_utils::base_elt, 614
readable
 rpki::https::http_stream, 282
reason
 rpki::https::http_response, 270
recipient
 rpki::up_down::message_pdu, 547
recv
 rpki::https::http_stream, 282
regen_margin
 rpki::left_right::self_elt, 347
regenerate
 rpki::rpki_engine::roa_obj, 476
regenerate_crls_and_manifests
 rpki::left_right::self_elt, 343
regexp
 rpki::sundial::timedelta, 514
reissue
 rpki::rpki_engine::child_cert_obj, 464
rekey
 rpki::rpki_engine::ca_obj, 459
relaxng.py(3110), 642
replace
 rpki::rpki_engine::publication_queue, 469
reply
 rpki::xml_utils::msg, 624
repositories
 rpki::left_right::bsc_elt, 293
rpki::left_right::self_elt, 343
rpki::rpki_engine::publication_queue, 469
repository
 rpki::left_right::parent_elt, 326
req_resource_set_as
 rpki::up_down::certificate_elt, 520
 rpki::up_down::issue_pdu, 536
req_resource_set_ipv4
 rpki::up_down::certificate_elt, 520
 rpki::up_down::issue_pdu, 536
req_resource_set_ipv6
 rpki::up_down::certificate_elt, 520
 rpki::up_down::issue_pdu, 536
request
 rpki::https::http_queue, 263
require_crls
 rpki::x509::CMS_object, 565
res
 rpki::async::sync_wrapper, 173
resource_set.py(3107), 642
resource_set_as
 rpki::up_down::class_elt, 524
resource_set_ipv4
 rpki::up_down::class_elt, 524
resource_set_ipv6
 rpki::up_down::class_elt, 524
resource_set_notafter
 rpki::up_down::class_elt, 524
resource_set_type
 rpki::resource_set::roa_prefix_set_ipv4, 435
 rpki::resource_set::roa_prefix_set_ipv6, 437
restart
 rpki::https::http_queue, 264
 rpki::https::http_stream, 283
result
 rpki::xml_utils::sax_handler, 628
retry
 rpki::https::http_request, 268
retry_read
 rpki::https::http_client, 254
 rpki::https::http_server, 275
 rpki::https::http_stream, 284
retry_write

rpkii::https::http_client, 254
rpkii::https::http_server, 275
rpkii::https::http_stream, 284
return_result
 rpkii::https::http_queue, 264
revoke
 rpkii::rpki_engine::ca_detail_obj,
 450
 rpkii::rpki_engine::ca_obj, 459
 rpkii::rpki_engine::child_cert_obj,
 464
 rpkii::rpki_engine::revoked_cert_obj,
 471
 rpkii::rpki_engine::roa_obj, 476
revoked
 rpkii::rpki_engine::revoked_cert_obj,
 472
revoked_certs
 rpkii::rpki_engine::ca_detail_obj,
 451
roa
 rpkii::rpki_engine::roa_obj, 479
roa.py(2424), 643
roas
 rpkii::left_right::self_elt, 343
 rpkii::rpki_engine::ca_detail_obj,
 451
root_newer_than_subject
 rootd, 58
rootd, 55
 bpki_ta, 59
 cfg, 59
 cfg_file, 59
 child_bpki_cert, 59
 client_ta, 59
 compose_response, 57
 del_subject_cert, 57
 del_subject_pkcs10, 57
 get_root_cert, 57
 get_subject_cert, 58
 get_subject_pkcs10, 58
 handlers, 59
 host, 59
 https_server_host, 60
 https_server_port, 60
 issue_subject_cert_maybe, 58
port, 60
root_newer_than_subject, 58
rootd_bpki_cert, 60
rootd_bpki_crl, 60
rootd_bpki_key, 60
rpki_base_uri, 60
rpki_class_name, 61
rpki_root_cert, 61
rpki_root_cert_file, 61
rpki_root_cert_uri, 61
rpki_root_crl, 61
rpki_root_dir, 61
rpki_root_key, 61
rpki_root_manifest, 62
rpki_subject_cert, 62
rpki_subject_lifetime, 62
rpki_subject_pkcs10, 62
rpki_subject_regen, 62
server_cert, 62
set_subject_cert, 58
set_subject_pkcs10, 58
up_down_handler, 58
rootd.py(2913), 644
rootd::cms_msg, 153
 saxify, 155
rootd::issue_pdu, 155
 serve_pdu, 157
rootd::list_pdu, 157
 serve_pdu, 159
rootd::message_pdu, 159
 log_query, 161
 name2type, 161
 type2name, 161
rootd::revoke_pdu, 162
 serve_pdu, 163
rootd::sax_handler, 163
 pdu, 165
rootd_bpki_cert
 rootd, 60
rootd_bpki_crl
 rootd, 60
rootd_bpki_key
 rootd, 60
rpki, 63
rpki.__doc__, 63
rpki.async, 63

rpki.cli, 66
rpki.config, 67
rpki.exceptions, 68
rpki.https, 70
rpki.ipaddrs, 75
rpki.left_right, 76
rpki.log, 77
rpki.manifest, 80
rpki.oids, 81
rpki.publication, 83
rpki.relaxng, 84
rpki.resource_set, 84
rpki.roa, 87
rpki.rpki_engine, 88
rpki.sql, 89
rpki.sundial, 90
rpki.up_down, 92
rpki.x509, 93
rpki.xml_utils, 95
rpki::async
 _raiseExitNow, 64
 defer, 64
 deferred_queue, 65
 event_loop, 65
 exit_event_loop, 65
 ExitNow, 65
 run_deferred, 65
rpki::async::gc_summary, 165
 __init__, 166
 handler, 166
 interval, 166
 threshold, 166
 timer, 166
rpki::async::iterator, 167
 __call__, 168
 __init__, 168
 __repr__, 169
 caller_function, 169
 doit, 169
 done_callback, 169
 item_callback, 169
 iterator, 169
 unwind_stack, 170
rpki::async::sync_wrapper, 170
 __call__, 172
 __init__, 172
 cb, 172
 eb, 172
 err, 173
 func, 173
 res, 173
rpki::async::timer, 173
 __cmp__, 176
 __del__, 176
 __init__, 176
 __repr__, 176
 cancel, 176
 clear, 176
 errback, 176, 178
 gc_debug, 178
 handler, 177, 179
 is_set, 177
 queue, 179
 run_debug, 179
 runq, 177
 seconds_until_wakeup, 177
 set, 177
 set_errback, 178
 set_handler, 178
 trace, 178
 when, 179
rpki::cli
 __yes_or_no_prompts, 67
 have_readline, 67
 yes_or_no, 66
rpki::cli::Cmd, 179
 __init__, 181
 cmdloop_with_history, 181, 183
 complete_help, 181
 completename, 182
 do_EOF, 182
 do_exit, 182
 do_quit, 183
 emptyline, 182
 emptyline_repeats_last_command,
 183
 EOF_exits_command_loop, 184
 filename_complete, 182
 help_help, 183
 histfile, 184
 identchars, 184
 onecmd, 183

rpk::config::parser, 184
 __init__, 186
 _reEXP, 188
 _repl, 186
 cfg, 188
 default_section, 189
 filename, 189
 get, 187
 getboolean, 187
 getint, 187
 getlong, 187
 has_option, 187
 has_section, 188
 multiget, 188
 set_global_flags, 188
rpk::exceptions::BadClassNameSyntax, 189
rpk::exceptions::BadClientURL, 190
rpk::exceptions::BadContactURL, 191
rpk::exceptions::BadExtension, 192
rpk::exceptions::BadIRDBReply, 193
rpk::exceptions::BadIssueResponse, 194
rpk::exceptions::BadPKCS10, 195
rpk::exceptions::BadPublicationReply, 196
 rpk::exceptions::BadQuery, 197
 rpk::exceptions::BadSender, 198
 rpk::exceptions::BadStatusCode, 199
 rpk::exceptions::BadURISyntax, 200
 rpk::exceptions::BSCNotFound, 201
 rpk::exceptions::BSCNotReady, 202
 rpk::exceptions::ChildNotFound, 203
 rpk::exceptions::ClassNameMismatch, 204
 rpk::exceptions::ClassNameUnknown, 205
 rpk::exceptions::ClientNotFound, 206
 rpk::exceptions::CMSContentNotSet, 207
 rpk::exceptions::CMSCRLNotSet, 209
 rpk::exceptions::CMSVerificationFailed, 210
 rpk::exceptions::DBConsistencyError, 211
 rpk::exceptions::DERObjectConversionError, 212
rpk::exceptions::DuplicateObject, 213
rpk::exceptions::EmptyPEM, 214
rpk::exceptions::EmptyROAPrefixList, 215
rpk::exceptions::ForbiddenURI, 216
rpk::exceptions::HandleTranslationError, 217
rpk::exceptions::HTTPRequestFailed, 218
rpk::exceptions::HTTPPSBadVersion, 219
rpk::exceptions::HTTPPSClientAborted, 220
rpk::exceptions::HTTPSUnexpectedState, 221
rpk::exceptions::MissingCMSCRL, 222
rpk::exceptions::MissingCMSEcert, 223
rpk::exceptions::MultipleTLSEECert, 224
rpk::exceptions::MustBePrefix, 225
rpk::exceptions::NoActiveCA, 226
rpk::exceptions::NoCoveringCertForROA, 227
rpk::exceptions::NoObjectAtURI, 228
rpk::exceptions::NotACertificateChain, 229
rpk::exceptions::NotFound, 230
rpk::exceptions::NotImplementedYet, 231
rpk::exceptions::NotInDatabase, 232
rpk::exceptions::ReceivedTLSACert, 233
rpk::exceptions::RPKI_Exception, 235
rpk::exceptions::ServerShuttingDown, 236
rpk::exceptions::SKIMismatch, 237
rpk::exceptions::SubprocessError, 238
rpk::exceptions::TLSValidation, 239
rpk::exceptions::UnexpectedCMSCerts, 241
rpk::exceptions::UnexpectedCMSCRLs, 242
rpk::exceptions::UnparsableCMSDER, 243
rpk::exceptions::UpstreamError, 244

rpki::exceptions::WrongEContentType, 245
rpki::https
 build_https_ta_cache, 72
 client, 72
 client_queues, 73
 debug_http, 73
 debug_tls_certs, 73
 default_client_timeout, 73
 default_http_version, 73
 default_server_timeout, 73
 log_method, 72
 rpki_content_type, 74
 server, 72
 supported_address_families, 74
 want_persistent_client, 74
 want_persistent_server, 74
rpki::https::caller, 246
 __call__, 247
 __init__, 247
 client_cert, 247
 client_key, 247
 debug, 248
 proto, 248
 server_cert, 248
 server_ta, 248
 url, 248
rpki::https::http_client, 248
 __init__, 250
 af, 253
 cert, 253
 expect_close, 253
 handle_close, 250
 handle_connect, 251
 handle_error, 251
 handle_message, 251
 handle_no_content_length, 251
 handle_timeout, 252
 hostport, 253
 key, 253
 parse_type, 253
 queue, 254
 retry_read, 254
 retry_write, 254
 send_request, 252
 set_state, 252
 start, 252
 state, 254
 ta, 254
 timeout, 254
 tls, 254
 tls_connect, 252
rpki::https::http_listener, 255
 __init__, 256
 cert, 257
 dynamic_ta, 257
 handle_accept, 256
 handle_error, 256
 handlers, 257
 key, 257
 log, 257
 ta, 257
rpki::https::http_message, 258
 __init__, 259
 __str__, 259
 body, 261
 format, 259
 headers, 261
 normalize_headers, 260
 parse_from_wire, 260
 parse_version, 260
 persistent, 260
 software_name, 261
 version, 261
rpki::https::http_queue, 261
 __init__, 263
 cert, 264
 client, 264
 detach, 263
 hostport, 265
 key, 265
 log, 265
 queue, 265
 request, 263
 restart, 264
 return_result, 264
 send_request, 264
 ta, 265
rpki::https::http_request, 265
 __init__, 267
 callback, 268
 cmd, 268

errback, 268
format_first_line, 267
parse_first_line, 267
path, 268
retried, 268
rpki::https::http_response, 268
 __init__, 270
 code, 270
 format_first_line, 270
 parse_first_line, 270
 reason, 270
rpki::https::http_server, 271
 __init__, 273
 expect_close, 275
 find_handler, 273
 handle_message, 273
 handle_no_content_length, 274
 handlers, 275
 parse_type, 275
 retry_read, 275
 retry_write, 275
 send_error, 274
 send_message, 274
 send_reply, 274
 timeout, 276
 tls, 276
 tls_accept, 274
rpki::https::http_stream, 276
 __init__, 279
 buffer, 284
 chunk_body, 279
 chunk_discard_crlf, 279
 chunk_discard_trailer, 279
 chunk_handler, 284
 chunk_header, 279
 close, 279
 collect_incoming_data, 280
 found_terminator, 280
 get_buffer, 280
 handle_body, 280
 handle_close, 281
 handle_error, 281
 handle_read, 281
 handle_timeout, 281
 handle_write, 282
 initiate_send, 282
log, 284
log_cert, 282
msg, 284
readable, 282
recv, 282
restart, 283
retry_read, 284
retry_write, 284
send, 283
timer, 284
tls, 285
update_timeout, 283
writeable, 283
rpki::ipaddrs::v4addr, 285
 __new__, 286
 __str__, 286
 bits, 287
 from_bytes, 286
 to_bytes, 286
rpki::ipaddrs::v6addr, 287
 __new__, 289
 __str__, 289
 bits, 289
 from_bytes, 289
 to_bytes, 289
rpki::left_right
 enforce_strict_up_down_xml_-
 sender, 77
rpki::left_right::bsc_elt, 290
 attributes, 293
 booleans, 293
 children, 292
 element_name, 294
 elements, 294
 handles, 294
 parents, 292
 pkcs10_request, 294
 private_key_id, 294
 repositories, 293
 serve_pre_save_hook, 293
 signing_cert, 294
 signing_cert_crl, 295
 sql_template, 295
rpki::left_right::child_elt, 295
 attributes, 299
 booleans, 299

bpkı_cert, 299
bpkı_glue, 299
ca_from_class_name, 297
child_certs, 297
clear_https_ta_cache, 299
element_name, 299
elements, 300
endElement, 298
handles, 300
parents, 298
serve_destroy_hook, 298
serve_post_save_hook, 298
serve_up_down, 298
sql_template, 300
rpkı:left_right::cms_msg, 300
encoding, 302
saxify, 302
schema, 302
rpkı:left_right::data_elt, 302
bsc, 304
handles, 306
make_reply_clone_hook, 304
self, 304
self_handle, 306
self_id, 306
serve_fetch_all, 305
serve_fetch_handle, 305
serve_fetch_one_maybe, 305
serve_pre_save_hook, 305
rpkı:left_right::left_right_namespace, 306
nsmap, 307
xmlns, 307
rpkı:left_right::list_published_objects_-
elt, 308
attributes, 311
element_name, 311
make_reply, 310
obj, 311
serve_dispatch, 310
text_attribute, 311
rpkı:left_right::list_received_resources_-
elt, 311
attributes, 313
element_name, 313
make_reply, 313
serve_dispatch, 313
rpkı:left_right::list_resources_elt, 314
asn, 317
attributes, 317
element_name, 317
ipv4, 317
ipv6, 317
startElement, 316
toXML, 316
valid_until, 317
rpkı:left_right::list_roa_requests_elt, 318
attributes, 319
element_name, 319
ipv4, 320
ipv6, 320
startElement, 319
rpkı:left_right::msg, 320
pdus, 322
serve_top_level, 322
version, 322
rpkı:left_right::parent_elt, 323
attributes, 327
booleans, 327
bpki_cms_cert, 327
bpki_cms_glue, 327
bpki_https_cert, 328
bpki_https_glue, 328
cas, 325
element_name, 328
elements, 328
handles, 328
query_up_down, 325
repository, 326
serve_post_save_hook, 326
serve_rekey, 326
serve_revoke, 326
serve_revoke_forgotten, 326
sql_template, 328
rpkı:left_right::report_error_elt, 329
attributes, 332
element_name, 332
error_code, 332
error_text, 332
from_exception, 331
self_handle, 332
tag, 332

text_attribute, 332
rpki::left_right::repository_elt, 333
 attributes, 336
 bpki_cert, 336
 bpki_glue, 336
 call_pubd, 335
 default_pubd_handler, 335
 element_name, 336
 elements, 337
 handles, 337
 parents, 336
 sql_template, 337
rpki::left_right::sax_handler, 337
 name, 339
 pdu, 339
 version, 339
rpki::left_right::self_elt, 339
 attributes, 346
 booleans, 346
 bpki_cert, 346
 bpki_glue, 346
 bscs, 342
 children, 342
 client_poll, 342
 crl_interval, 347
 cron, 342
 element_name, 347
 elements, 347
 handles, 347
 parents, 342
 regen_margin, 347
 regenerate_crls_and_manifests, 343
 repositories, 343
 roas, 343
 serve_fetch_all, 343
 serve_fetch_handle, 344
 serve_fetch_one_maybe, 344
 serve_post_save_hook, 344
 serve_publish_world_now, 344
 serve_rekey, 345
 serve_revocate, 345
 serve_revoke_forgotten, 345
 serve_run_now, 345
 sql_template, 347
 update_children, 345
 update_roas, 346
use_hsm, 348
rpki::log
 debug, 79
 enable_trace, 79
 error, 79
 info, 79
 init, 78
 note, 80
 pid, 80
 set_trace, 78
 tag, 80
 trace, 79
 traceback, 79
 use_syslog, 80
 warn, 80
rpki::log::logger, 348
 __call__, 349
 __init__, 349
 priority, 349
rpki::manifest::FileAndHash, 350
 __init__, 351
 file, 351
 hash, 351
rpki::manifest::FilesAndHashes, 351
 __init__, 352
rpki::manifest::Manifest, 353
 __init__, 354
 explicitVersion, 354
 fileHashAlg, 354
 fileList, 354
 manifestNumber, 354
 nextUpdate, 354
 thisUpdate, 355
 version, 355
rpki::oids
 name2oid, 82
 oid2name, 82
rpki::publication::certificate_elt, 355
 element_name, 357
 payload_type, 357
rpki::publication::client_elt, 357
 attributes, 360
 base_uri, 360
 bpki_cert, 361
 bpki_glue, 361
 check_allowed_uri, 359

clear_https_ta_cache, 361
element_name, 361
elements, 361
endElement, 359
serve_fetch_all, 360
serve_fetch_one_maybe, 360
serve_post_save_hook, 360
sql_template, 361
rpki::publication::cms_msg, 362
encoding, 364
saxify, 364
schema, 364
rpki::publication::config_elt, 364
attributes, 367
config_id, 367
element_name, 368
elements, 368
fetch, 366
serve_fetch_one_maybe, 366
serve_set, 367
sql_template, 368
startElement, 367
wired_in_config_id, 368
rpki::publication::control_elt, 368
serve_dispatch, 371
rpki::publication::crl_elt, 371
element_name, 373
payload_type, 373
rpki::publication::manifest_elt, 373
element_name, 375
payload_type, 375
rpki::publication::msg, 375
pdus, 377
serve_top_level, 377
version, 377
rpki::publication::publication_-
 namespace, 378
 nsmap, 379
 xmlns, 379
rpki::publication::publication_object_elt,
 379
 attributes, 383
 endElement, 381
 make_publish, 381
 make_withdraw, 382
 payload, 383
payload_type, 383
raise_if_error, 382
serve_dispatch, 382
serve_publish, 382
serve_withdraw, 382
toXML, 383
uri_to_filename, 383
rpki::publication::report_error_elt, 384
__str__, 386
attributes, 387
element_name, 387
error_code, 387
error_text, 387
from_exception, 386
raise_if_error, 387
tag, 388
text_attribute, 388
rpki::publication::roa_elt, 388
element_name, 390
payload_type, 390
rpki::publication::sax_handler, 390
name, 392
pdu, 392
version, 392
rpki::relaxng
 left_right, 84
 publication, 84
 up_down, 84
rpki::resource_set
 _bs2long, 86
 _long2bs, 86
 _rsplit, 86
 inherit_token, 87
 test1, 87
 test2, 87
rpki::resource_set::resource_bag, 392
 __eq__, 394
 __init__, 394
 __ne__, 394
 __str__, 395
 asn, 396
 empty, 395
 from_rfc3779_tuples, 395
 intersection, 395
 oversized, 395
 undersized, 395

union, 396
v4, 396
v6, 396
valid_until, 396
rpki::resource_set::resource_range, 397
 __cmp__, 398
 __init__, 398
 max, 398
 min, 398
rpki::resource_set::resource_range_as, 399
 __str__, 400
 datum_type, 400
 min, 401
 to_rfc3779_tuple, 400
rpki::resource_set::resource_range_ip, 401
 __str__, 403
 _prefixlen, 403
 make_prefix, 403
 to_rfc3779_tuple, 403
rpki::resource_set::resource_range_ipv4, 404
 datum_type, 406
rpki::resource_set::resource_range_ipv6, 406
 datum_type, 408
rpki::resource_set::resource_set, 408
 __init__, 410
 __str__, 410
 _comm, 410
 contains, 411
 difference, 411
 from_sql, 411
 inherit, 412
 intersection, 411
 issubset, 411
 issuperset, 412
 symmetric_difference, 412
 union, 412
rpki::resource_set::resource_set_as, 413
 inherit, 415
 parse_rfc3779_tuple, 414
 parse_str, 414
 range_type, 415
 to_rfc3779_tuple, 414
rpki::resource_set::resource_set_ip, 415
 inherit, 418
 parse_rfc3779_tuple, 417
 parse_str, 417
 to_rfc3779_tuple, 417
rpki::resource_set::resource_set_ipv4, 418
 afi, 420
 range_type, 420
rpki::resource_set::resource_set_ipv6, 420
 afi, 422
 range_type, 422
rpki::resource_set::roa_prefix, 422
 __cmp__, 424
 __init__, 424
 __str__, 424
 max, 424
 max_prefixlen, 425
 min, 425
 prefix, 425
 prefixlen, 426
 to_resource_range, 425
 to_roa_tuple, 425
rpki::resource_set::roa_prefix_ipv4, 426
 range_type, 428
rpki::resource_set::roa_prefix_ipv6, 428
 range_type, 430
rpki::resource_set::roa_prefix_set, 430
 __init__, 432
 __str__, 432
 from_sql, 432
 parse_str, 432
 to_resource_set, 432
 to_roa_tuple, 433
rpki::resource_set::roa_prefix_set_ipv4, 433
 prefix_type, 435
 resource_set_type, 435
rpki::resource_set::roa_prefix_set_ipv6, 435
 prefix_type, 437
 resource_set_type, 437
rpki::roa::ROAIPAddress, 437
 __init__, 438
 address, 439

maxLength, 439
rpki::roa::ROAIPAddresses, 439
 __init__, 440
rpki::roa::ROAIPAddressFamilies, 440
 __init__, 441
rpki::roa::ROAIPAddressFamily, 441
 __init__, 442
 addresses, 443
 addressFamily, 443
rpki::roa::RouteOriginAttestation, 443
 __init__, 444
 asID, 444
 explicitVersion, 444
 ipAddrBlocks, 444
 version, 444
rpki::rpki_engine::ca_detail_obj, 445
 activate, 448
 ca, 448
 ca_cert_uri, 452
 ca_id, 452
 child_certs, 448
 create, 448
 crl_published, 452
 crl_published_callback, 448
 crl_uri, 448
 crl_uri_tail, 449
 delete, 449
 gctx, 452
 generate_crl, 449
 generate_manifest, 449
 generate_manifest_cert, 449
 issue, 450
 issue_ee, 450
 latest_ca_cert, 452
 latest_crl, 452
 latest_manifest, 453
 latest_manifest_cert, 453
 manifest_private_key_id, 453
 manifest_public_key, 453
 manifest_published, 453
 manifest_published_callback, 450
 manifest_uri, 450
 nextUpdate, 453
 private_key_id, 453
 public_key, 454
 revoke, 450
 revoked_certs, 451
 roas, 451
 sql_decode, 451
 sql_template, 454
 state, 454
 update, 451
rpki::rpki_engine::ca_obj, 454
 ca_details, 456
 check_for_updates, 456
 construct_sia_uri, 457
 create, 457
 delete, 457
 fetch_active, 457
 fetch_DEPRECATED, 458
 fetch_issue_response_candidates, 458
 fetch_pending, 458
 fetch_revoked, 458
 gctx, 460
 last_crl_sn, 460
 last_issued_sn, 460
 last_manifest_sn, 460
 next_crl_number, 458
 next_manifest_number, 459
 next_serial_number, 459
 parent, 459
 parent_id, 460
 parent_resource_class, 460
 rekey, 459
 revoke, 459
 sia_uri, 461
 sql_template, 461
rpki::rpki_engine::child_cert_obj, 461
 __init__, 463
 ca_detail, 463
 ca_detail_id, 465
 cert, 465
 child, 463
 child_id, 465
 fetch, 464
 gctx, 465
 published, 465
 published_callback, 464
 reissue, 464
 revoke, 464
 sql_template, 466

uri, 464
uri_tail, 465
rpki::rpki_engine::publication_queue,
 466
 __init__, 468
 _add, 468
 call_pubd, 468
 handlers, 469
 msgs, 469
 publish, 468
 replace, 469
 repositories, 469
 uris, 469
 withdraw, 469
rpki::rpki_engine::revoked_cert_obj, 470
 __init__, 471
 ca_detail, 471
 ca_detail_id, 472
 expires, 472
 gctx, 472
 revoke, 471
 revoked, 472
 serial, 472
 sql_template, 472
rpki::rpki_engine::roa_obj, 473
 __init__, 475
 asn, 478
 ca_detail, 475
 ca_detail_id, 478
 cert, 478
 gctx, 479
 generate, 476
 ipv4, 479
 ipv6, 479
 published, 479
 published_callback, 476
 regenerate, 476
 revoke, 476
 roa, 479
 self, 477
 self_id, 479
 sql_delete_hook, 477
 sql_fetch_hook, 477
 sql_insert_hook, 477
 sql_template, 479
 update, 478
 uri, 478
 uri_tail, 478
 rpki::rpki_engine::rpkid_context, 480
 __init__, 483
 bpki_ta, 485
 build_https_ta_cache, 483
 checkpoint, 483
 clear_https_ta_cache, 483
 cron, 483
 cron_keepalive, 485
 cron_period, 485
 cron_timeout, 485
 cron_timer, 485
 cronjob_handler, 483
 https_server_host, 486
 https_server_port, 486
 https_ta_cache, 486
 initial_delay, 486
 irbe_cert, 486
 irdb_cert, 486
 irdb_query, 484
 irdb_query_child_resources, 484
 irdb_query_roa_requests, 484
 irdb_url, 486
 left_right_handler, 484
 publication_kludge_base, 487
 rpkid_cert, 487
 rpkid_key, 487
 sql, 487
 start_cron, 484
 up_down_handler, 485
 up_down_url_regex, 487
 use_internal_cron, 487
rpki::sql::session, 488
 __init__, 490
 _exceptions_enabled, 491
 _wrap_execute, 490
 assert_pristine, 490
 cache, 492
 cache_clear, 490
 close, 490
 connect, 490
 cur, 492
 database, 492
 db, 492
 dirty, 492

execute, 490
executemany, 491
fetchall, 491
lastrowid, 491
password, 492
ping, 491
sweep, 491
username, 492
rpki::sql::sql_persistent, 493
 gctx, 499
 sql_debug, 499
 sql_decode, 495
 sql_delete, 496
 sql_delete_hook, 496
 sql_deleted, 499
 sql_encode, 496
 sql_fetch, 496
 sql_fetch_all, 497
 sql_fetch_hook, 497
 sql_fetch_where, 497
 sql_fetch_where1, 497
 sql_in_db, 500
 sql_init, 497
 sql_insert_hook, 498
 sql_is_dirty, 498
 sql_mark_clean, 498
 sql_mark_deleted, 498
 sql_mark_dirty, 498
 sql_store, 499
 sql_update_hook, 499
rpki::sql::template, 500
 __init__, 502
 columns, 502
 delete, 502
 index, 502
 insert, 502
 map, 503
 select, 503
 table, 503
 update, 503
rpki::sundial
 _cast, 91
 now, 91
 test, 91
rpki::sundial::datetime, 503
 __add__, 505
 __radd__, 505
 __rsub__, 505
 __str__, 506
 __sub__, 506
 earlier, 506
 from_sql, 506
 fromASN1tuple, 506
 fromdatetime, 506
 fromGeneralizedTime, 507
 fromUTCTime, 507
 fromXMLtime, 507
 later, 507
 PKIX_threshhold, 509
 to_sql, 507
 toASN1tuple, 508
 toGeneralizedTime, 508
 totimestamp, 508
 toUTCTime, 508
 toXMLtime, 508
rpki::sundial::timedelta, 509
 __abs__, 512
 __add__, 512
 __div__, 512
 __floordiv__, 512
 __mul__, 512
 __neg__, 512
 __pos__, 512
 __radd__, 512
 __rdiv__, 513
 __rfloordiv__, 513
 __rmul__, 513
 __rsub__, 513
 __sub__, 513
 convert_to_seconds, 513
 fromtimedelta, 513
 parse, 514
 regexp, 514
 years_to_seconds, 514
rpki::up_down
 nsmap, 93
 xmlns, 93
rpki::up_down::base_elt, 515
 check_response, 516
 endElement, 516
 make_b64elt, 516
 make_elt, 516

serve_pdu, 517
startElement, 517
rpki::up_down::certificate_elt, 517
cert, 520
cert_url, 520
endElement, 519
req_resource_set_as, 520
req_resource_set_ipv4, 520
req_resource_set_ipv6, 520
startElement, 519
toXML, 519
rpki::up_down::class_elt, 520
__init__, 522
cert_url, 523
certs, 523
class_name, 523
endElement, 522
from_resource_bag, 522
issuer, 524
resource_set_as, 524
resource_set_ipv4, 524
resource_set_ipv6, 524
resource_set_notafter, 524
startElement, 523
suggested_sia_head, 524
to_resource_bag, 523
toXML, 523
rpki::up_down::class_response_syntax,
 525
 __init__, 526
 classes, 527
 startElement, 526
 toXML, 526
rpki::up_down::cms_msg, 527
 encoding, 529
 saxify, 529
 schema, 529
rpki::up_down::error_response_pdu, 529
 __init__, 531
 check_response, 531
 codes, 532
 description, 532
 endElement, 531
 exceptions, 532
 status, 532
 toXML, 532
rpki::up_down::issue_pdu, 533
 class_name, 536
 endElement, 535
 pkcs10, 536
 query, 535
 req_resource_set_as, 536
 req_resource_set_ipv4, 536
 req_resource_set_ipv6, 536
 serve_pdu, 535
 startElement, 535
 toXML, 536
rpki::up_down::issue_response_pdu, 537
 check_response, 539
rpki::up_down::list_pdu, 539
 query, 541
 serve_pdu, 541
 toXML, 541
rpki::up_down::list_response_pdu, 542
rpki::up_down::message_pdu, 543
 __str__, 545
 log_query, 545
 make_query, 545
 name2type, 547
 payload, 547
 recipient, 547
 sender, 547
 serve_error, 546
 serve_top_level, 546
 startElement, 546
 toXML, 546
 type, 547
 type2name, 547
 version, 548
rpki::up_down::multi_uri, 548
 __init__, 549
 __str__, 550
 rsync, 550
rpki::up_down::revoke_pdu, 550
 class_name, 553
 get_SKI, 552
 query, 552
 serve_pdu, 552
 ski, 553
rpki::up_down::revoke_response_pdu,
 553
rpki::up_down::revoke_syntax, 555

class_name, 556
 ski, 556
 startElement, 556
 toXML, 556
rpk:::up_down::sax_handler, 557
 name, 559
 pdu, 559
 version, 559
rpki:::x509
 _find_xia_uri, 95
 calculate_SKI, 95
 POWify_OID, 95
rpki:::x509::CMS_object, 559
 content, 563
 debug_cms_certs, 563
 DER, 564
 dump_on_verify_failure, 564
 econtent_oid, 564
 extract, 562
 formats, 564
 get_content, 562
 get_DER, 562
 get_POW, 562
 other_clear, 564
 pem_converter, 565
 POW, 565
 print_on_der_error, 565
 require_crls, 565
 set_content, 563
 sign, 563
 verify, 563
rpki:::x509::CRL, 566
 DER, 569
 formats, 569
 generate, 567
 get_DER, 567
 get_POW, 568
 get_POWpkix, 568
 getIssuer, 568
 getNextUpdate, 568
 getThisUpdate, 568
 pem_converter, 569
 POW, 569
 POWpkix, 569
rpki:::x509::DeadDrop, 570
 __init__, 571
 dump, 571
 maildir, 571
 pid, 571
 rpki:::x509::DER_CMS_object, 572
 content, 573
 decode, 573
 encode, 573
 rpki:::x509::DER_object, 574
 __cmp__, 576
 __init__, 576
 clear, 576
 DER, 581
 dumpasn1, 576
 empty, 576
 formats, 581
 from_sql, 577
 gAKI, 577
 get_3779resources, 577
 get_AIA, 577
 get_aia_uri, 577
 get_AKI, 578
 get_Base64, 578
 get_basicConstraints, 578
 get_DER, 578
 get_PEM, 578
 get_SIA, 579
 get_sia_directory_uri, 579
 get_sia_manifest_uri, 579
 get_SKI, 579
 gSKI, 579
 hAKI, 580
 hSKI, 580
 is_CA, 580
 other_clear, 581
 pem_converter, 581
 set, 580
 to_sql, 580
 rpki:::x509::PEM_converter, 582
 __init__, 583
 b, 584
 e, 584
 looks_like_PEM, 583
 to_DER, 583
 to_PEM, 583
 rpki:::x509::PKCS10, 584
 check_valid_rpki, 586

create, 586
create_ca, 586
DER, 587
formats, 587
get_DER, 587
get_POWpkix, 587
getPublicKey, 587
pem_converter, 588
POWpkix, 588
rpki::x509::ROA, 588
build, 590
content_class, 590
econtent_oid, 590
pem_converter, 590
rpki::x509::RSA, 591
DER, 594
formats, 594
generate, 593
get_DER, 593
get_POW, 593
get_public_DER, 594
get_RSAPublic, 594
get_SKI, 594
pem_converter, 595
POW, 595
rpki::x509::RSAPublic, 595
DER, 598
formats, 598
get_DER, 597
get_POW, 597
get_SKI, 597
pem_converter, 598
POW, 598
rpki::x509::SignedManifest, 599
build, 600
content_class, 601
econtent_oid, 601
getNextUpdate, 600
getThisUpdate, 600
pem_converter, 601
rpki::x509::X509, 601
cross_certify, 603
DER, 606
expired, 604
formats, 606
get_DER, 604
get_POW, 604
get_POWpkix, 604
getIssuer, 604
getNotAfter, 604
getNotBefore, 605
getPublicKey, 605
getSerial, 605
getSubject, 605
issue, 605
normalize_chain, 606
pem_converter, 606
POW, 607
POWpkix, 607
rpki::x509::XML_CMS_object, 607
content, 611
decode, 609
dump_inbound_cms, 611
dump_outbound_cms, 611
dump_to_disk, 609
econtent_oid, 611
encode, 609
pretty_print_content, 610
schema_check, 610
unwrap, 610
wrap, 610
rpki::xml_utils::base_elt, 611
__str__, 613
attributes, 615
booleans, 615
elements, 615
endElement, 613
make_b64elt, 614
make_elt, 614
make_pdu, 614
readAttrs, 614
startElement, 614
toXML, 615
rpki::xml_utils::data_elt, 616
endElement, 618
make_reply, 618
make_reply_clone_hook, 618
serve_create, 619
serve_destroy, 619
serve_destroy_hook, 619
serve_dispatch, 619
serve_fetch_one, 619

serve_get, 620
serve_list, 620
serve_post_save_hook, 620
serve_pre_save_hook, 620
serve_set, 620
toXML, 621
unimplemented_control, 621
rpki::xml_utils::msg, 621
 __str__, 623
 endElement, 623
 is_query, 623
 is_reply, 623
 query, 623
 reply, 624
 startElement, 624
 toXML, 624
 type, 624
 version, 624
rpki::xml_utils::sax_handler, 625
 __init__, 626
 characters, 626
 create_top_level, 627
 endElement, 627
 endElementNS, 627
 result, 628
 saxify, 627
 stack, 628
 startElement, 627
 startElementNS, 628
 text, 628
rpki::xml_utils::text_elt, 629
 endElement, 630
 text_attribute, 630
 toXML, 630
rpki_base_uri
 rootd, 60
rpki_class_name
 rootd, 61
rpki_content_type
 rpki::https, 74
rpki_engine.py(3107), 645
rpki_root_cert
 rootd, 61
rpki_root_cert_file
 rootd, 61
rpki_root_cert_uri
 rootd, 61
rpki_root_crl
 rootd, 61
rpki_root_dir
 rootd, 61
rpki_root_key
 rootd, 61
rpki_root_manifest
 rootd, 62
rpki_subject_cert
 rootd, 62
rpki_subject_lifetime
 rootd, 62
rpki_subject_pkcs10
 rootd, 62
rpki_subject_regen
 rootd, 62
rpkid, 96
 cfg_file, 97
 main, 97
 profile, 97
rpkid.py(2913), 646
rpkid_cert
 irdbd, 53
 rpki::rpki_engine::rpkid_context,
 487
rpkid_key
 rpki::rpki_engine::rpkid_context,
 487
rsync
 rpki::up_down::multi_uri, 550
run_debug
 rpki::async::timer, 179
run_deferred
 rpki::async, 65
runq
 rpki::async::timer, 177
saxify
 irbe_cli::left_right_cms_msg, 118
 irbe_cli::publication_cms_msg, 133
 rootd::cms_msg, 155
 rpki::left_right::cms_msg, 302
 rpki::publication::cms_msg, 364
 rpki::up_down::cms_msg, 529
 rpki::xml_utils::sax_handler, 627

schema
 rpki::left_right::cms_msg, 302
 rpki::publication::cms_msg, 364
 rpki::up_down::cms_msg, 529
schema_check
 rpki::x509::XML_CMS_object, 610
seconds_until_wakeup
 rpki::async::timer, 177
select
 rpki::sql::template, 503
self
 rpki::left_right::data_elt, 304
 rpki::rpk_engine::roa_obj, 477
self_handle
 rpki::left_right::data_elt, 306
 rpki::left_right::report_error_elt, 332
self_id
 rpki::left_right::data_elt, 306
 rpki::rpk_engine::roa_obj, 479
send
 rpki::https::http_stream, 283
send_error
 rpki::https::http_server, 274
send_message
 rpki::https::http_server, 274
send_reply
 rpki::https::http_server, 274
send_request
 rpki::https::http_client, 252
 rpki::https::http_queue, 264
sender
 rpki::up_down::message_pdu, 547
Sequence, 631
SequenceOf, 631
serial
 rpki::rpk_engine::revoked_cert_obj, 472
serve_create
 rpki::xml_utils::data_elt, 619
serve_destroy
 rpki::xml_utils::data_elt, 619
serve_destroy_hook
 rpki::left_right::child_elt, 298
 rpki::xml_utils::data_elt, 619
serve_dispatch
 rpki::left_right::list_published_objects_elt, 310
 rpki::left_right::list_received_resources_elt, 313
 rpki::publication::control_elt, 371
 rpki::publication::publication_object_elt, 382
 rpki::xml_utils::data_elt, 619
serve_error
 rpki::up_down::message_pdu, 546
serve_fetch_all
 rpki::left_right::data_elt, 305
 rpki::left_right::self_elt, 343
 rpki::publication::client_elt, 360
serve_fetch_handle
 rpki::left_right::data_elt, 305
 rpki::left_right::self_elt, 344
serve_fetch_one
 rpki::xml_utils::data_elt, 619
serve_fetch_one_maybe
 rpki::left_right::data_elt, 305
 rpki::left_right::self_elt, 344
 rpki::publication::client_elt, 360
 rpki::publication::config_elt, 366
serve_get
 rpki::xml_utils::data_elt, 620
serve_list
 rpki::xml_utils::data_elt, 620
serve_pdu
 rootd::issue_pdu, 157
 rootd::list_pdu, 159
 rootd::revoke_pdu, 163
 rpki::up_down::base_elt, 517
 rpki::up_down::issue_pdu, 535
 rpki::up_down::list_pdu, 541
 rpki::up_down::revoke_pdu, 552
serve_post_save_hook
 rpki::left_right::child_elt, 298
 rpki::left_right::parent_elt, 326
 rpki::left_right::self_elt, 344
 rpki::publication::client_elt, 360
 rpki::xml_utils::data_elt, 620
serve_pre_save_hook
 rpki::left_right::bsc_elt, 293
 rpki::left_right::data_elt, 305
 rpki::xml_utils::data_elt, 620

serve_publish
 rpki::publication::publication_object_elt, 382

serve_publish_world_now
 rpki::left_right::self_elt, 344

serve_rekey
 rpki::left_right::parent_elt, 326
 rpki::left_right::self_elt, 345

serve_revocate
 rpki::left_right::parent_elt, 326
 rpki::left_right::self_elt, 345

serve_revoke_forgotten
 rpki::left_right::parent_elt, 326
 rpki::left_right::self_elt, 345

serve_run_now
 rpki::left_right::self_elt, 345

serve_set
 rpki::publication::config_elt, 367
 rpki::xml_utils::data_elt, 620

serve_top_level
 rpki::left_right::msg, 322
 rpki::publication::msg, 377
 rpki::up_down::message_pdu, 546

serve_up_down
 rpki::left_right::child_elt, 298

serve_withdraw
 rpki::publication::publication_object_elt, 382

server
 rpki::https, 72

server_cert
 irdbd, 53
 rootd, 62
 rpki::https::caller, 248

server_ta
 rpki::https::caller, 248

set
 rpki::async::timer, 177
 rpki::x509::DER_object, 580

set_content
 rpki::x509::CMS_object, 563

set_errback
 rpki::async::timer, 178

set_global_flags
 rpki::config::parser, 188

set_handler

 rpki::async::timer, 178

set_state
 rpki::https::http_client, 252

set_subject_cert
 rootd, 58

set_subject_pkcs10
 rootd, 58

set_trace
 rpki::log, 78

sia_uri
 rpki::rpki_engine::ca_obj, 461

sign
 rpki::x509::CMS_object, 563

signing_cert
 irbe_cli::bsc_elt, 101
 rpki::left_right::bsc_elt, 294

signing_cert_crl
 irbe_cli::bsc_elt, 101
 rpki::left_right::bsc_elt, 295

ski
 rpki::up_down::revoke_pdu, 553
 rpki::up_down::revoke_syntax, 556

software_name
 rpki::https::http_message, 261

sql
 pubd::pubd_context, 153
 rpki::rpki_engine::rpkid_context, 487

sql.py(2895), 646

sql_debug
 rpki::sql::sql_persistent, 499

sql_decode
 rpki::rpki_engine::ca_detail_obj, 451
 rpki::sql::sql_persistent, 495

sql_delete
 rpki::sql::sql_persistent, 496

sql_delete_hook
 rpki::rpki_engine::roa_obj, 477
 rpki::sql::sql_persistent, 496

sql_deleted
 rpki::sql::sql_persistent, 499

sql_encode
 rpki::sql::sql_persistent, 496

sql_fetch
 rpki::sql::sql_persistent, 496

sql_fetch_all
 rpki::sql::sql_persistent, 497

sql_fetch_hook
 rpki::rpki_engine::roa_obj, 477
 rpki::sql::sql_persistent, 497

sql_fetch_where
 rpki::sql::sql_persistent, 497

sql_fetch_where1
 rpki::sql::sql_persistent, 497

sql_in_db
 rpki::sql::sql_persistent, 500

sql_init
 rpki::sql::sql_persistent, 497

sql_insert_hook
 rpki::rpki_engine::roa_obj, 477
 rpki::sql::sql_persistent, 498

sql_is_dirty
 rpki::sql::sql_persistent, 498

sql_mark_clean
 rpki::sql::sql_persistent, 498

sql_mark_deleted
 rpki::sql::sql_persistent, 498

sql_mark_dirty
 rpki::sql::sql_persistent, 498

sql_store
 rpki::sql::sql_persistent, 499

sql_template
 rpki::left_right::bsc_elt, 295
 rpki::left_right::child_elt, 300
 rpki::left_right::parent_elt, 328
 rpki::left_right::repository_elt, 337
 rpki::left_right::self_elt, 347
 rpki::publication::client_elt, 361
 rpki::publication::config_elt, 368
 rpki::rpki_engine::ca_detail_obj, 454
 rpki::rpki_engine::ca_obj, 461
 rpki::rpki_engine::child_cert_obj, 466
 rpki::rpki_engine::revoked_cert_obj, 472
 rpki::rpki_engine::roa_obj, 479

sql_update_hook
 rpki::sql::sql_persistent, 499

stack
 rpki::xml_utils::sax_handler, 628

start
 rpki::https::http_client, 252

start_cron
 rpki::rpki_engine::rpkid_context, 484

startElement
 rpki::left_right::list_resources_elt, 316

rpki::left_right::list_roa_requests_elt, 319

rpki::publication::config_elt, 367

rpki::up_down::base_elt, 517

rpki::up_down::certificate_elt, 519

rpki::up_down::class_elt, 523

rpki::up_down::class_response_syntax, 526

rpki::up_down::issue_pdu, 535

rpki::up_down::message_pdu, 546

rpki::up_down::revoke_syntax, 556

rpki::xml_utils::base_elt, 614

rpki::xml_utils::msg, 624

rpki::xml_utils::sax_handler, 627

startElementNS
 rpki::xml_utils::sax_handler, 628

startup_msg
 irdbd, 53

state
 rpki::https::http_client, 254
 rpki::rpki_engine::ca_detail_obj, 454

status
 rpki::up_down::error_response_pdu, 532

suggested_sia_head
 rpki::up_down::class_elt, 524

sundial.py(3191), 646

supported_address_families
 rpki::https, 74

sweep
 rpki::sql::session, 491

symmetric_difference
 rpki::resource_set::resource_set, 412

ta
 rpki::https::http_client, 254
 rpki::https::http_listener, 257

rpki::https::http_queue, 265
table rpki::sql::template, 503
tag rpki::left_right::report_error_elt, 332
rpki::log, 80
rpki::publication::report_error_elt, 388
test rpki::sundial, 91
test1 rpki::resource_set, 87
test2 rpki::resource_set, 87
text rpki::xml_utils::sax_handler, 628
text_attribute rpki::left_right::list_published_objects_elt, 311
rpki::left_right::report_error_elt, 332
rpki::publication::report_error_elt, 388
rpki::xml_utils::text_elt, 630
textwrap::TextWrapper, 631
thisUpdate rpki::manifest::Manifest, 355
threshold rpki::async::gc_summary, 166
timeout rpki::https::http_client, 254
rpki::https::http_server, 276
timer rpki::async::gc_summary, 166
rpki::https::http_stream, 284
tls rpki::https::http_client, 254
rpki::https::http_server, 276
rpki::https::http_stream, 285
tls_accept rpki::https::http_server, 274
tls_connect rpki::https::http_client, 252
to_bytes rpki::ipaddrs::v4addr, 286
rpki::ipaddrs::v6addr, 289
to_DER rpki::x509::PEM_converter, 583
to_PEM rpki::x509::PEM_converter, 583
to_resource_bag rpki::up_down::class_elt, 523
to_resource_range rpki::resource_set::roa_prefix, 425
to_resource_set rpki::resource_set::roa_prefix_set, 432
to_rfc3779_tuple rpki::resource_set::resource_range_as, 400
rpki::resource_set::resource_range_ip, 403
rpki::resource_set::resource_set_as, 414
rpki::resource_set::resource_set_ip, 417
to_roa_tuple rpki::resource_set::roa_prefix, 425
rpki::resource_set::roa_prefix_set, 433
to_sql rpki::sundial::datetime, 507
rpki::x509::DER_object, 580
toASN1tuple rpki::sundial::datetime, 508
toGeneralizedTime rpki::sundial::datetime, 508
top_opts irbe_cli, 48
totimestamp rpki::sundial::datetime, 508
toUTCTime rpki::sundial::datetime, 508
toXML rpki::left_right::list_resources_elt, 316
rpki::publication::publication_object_elt, 383
rpki::up_down::certificate_elt, 519
rpki::up_down::class_elt, 523
rpki::up_down::class_response_syntax, 526

rpki::up_down::error_response_pdu, 532
rpki::up_down::issue_pdu, 536
rpki::up_down::list_pdu, 541
rpki::up_down::message_pdu, 546
rpki::up_down::revoke_syntax, 556
rpki::xml_utils::base_elt, 615
rpki::xml_utils::data_elt, 621
rpki::xml_utils::msg, 624
rpki::xml_utils::text_elt, 630
toXMLtime
 rpki::sundial::datetime, 508
trace
 rpki::async::timer, 178
 rpki::log, 79
traceback
 rpki::log, 79
type
 rpki::up_down::message_pdu, 547
 rpki::xml_utils::msg, 624
type2name
 rootd::message_pdu, 161
 rpki::up_down::message_pdu, 547

u
 irdbd, 53

undersized
 rpki::resource_set::resource_bag, 395

unimplemented_control
 rpki::xml_utils::data_elt, 621

union
 rpki::resource_set::resource_bag, 396
 rpki::resource_set::resource_set, 412

unwind_stack
 rpki::async::iterator, 170

unwrap
 rpki::x509::XML_CMS_object, 610

up_down
 rpki::relaxng, 84

up_down.py(3162), 647

up_down_handler
 rootd, 58
 rpki::rpki_engine::rpkid_context, 485

up_down_url_regexp
 rpki::rpki_engine::rpkid_context, 487

update
 rpki::rpki_engine::ca_detail_obj, 451
 rpki::rpki_engine::roa_obj, 478
 rpki::sql::template, 503

update_children
 rpki::left_right::self_elt, 345

update_roas
 rpki::left_right::self_elt, 346

update_timeout
 rpki::https::http_stream, 283

uri
 rpki::rpki_engine::child_cert_obj, 464
 rpki::rpki_engine::roa_obj, 478

uri_tail
 rpki::rpki_engine::child_cert_obj, 465
 rpki::rpki_engine::roa_obj, 478

uri_to_filename
 rpki::publication::publication_object_elt, 383

uris
 rpki::rpki_engine::publication_queue, 469

url
 rpki::https::caller, 248

usage
 irbe_cli, 47
 irbe_cli::cmd_elt_mixin, 110
 irbe_cli::cmd_msg_mixin, 113

usage_fill
 irbe_cli, 49

use_hsm
 rpki::left_right::self_elt, 348

use_internal_cron
 rpki::rpki_engine::rpkid_context, 487

use_syslog
 rpki::log, 80

username
 rpki::sql::session, 492

v4
 rpki::resource_set::resource_bag,
 396

v6
 rpki::resource_set::resource_bag,
 396

valid_until
 rpki::left_right::list_resources_elt,
 317

 rpki::resource_set::resource_bag,
 396

verbose
 irbe_cli, 49

verify
 rpki::x509::CMS_object, 563

version
 rpki::https::http_message, 261
 rpki::left_right::msg, 322
 rpki::left_right::sax_handler, 339
 rpki::manifest::Manifest, 355
 rpki::publication::msg, 377
 rpki::publication::sax_handler, 392
 rpki::roa::RouteOriginAttestation,
 444
 rpki::up_down::message_pdu, 548
 rpki::up_down::sax_handler, 559
 rpki::xml_utils::msg, 624

want_persistent_client
 rpki::https, 74

want_persistent_server
 rpki::https, 74

warn
 rpki::log, 80

when
 rpki::async::timer, 179

wired_in_config_id
 rpki::publication::config_elt, 368

withdraw
 rpki::rpki_engine::publication_-
 queue, 469

wrap
 rpki::x509::XML_CMS_object, 610

writeable
 rpki::https::http_stream, 283