

# RPKI Engine

## 1.0

Generated by Doxygen 1.6.3

Thu Apr 15 15:51:08 2010

## Contents

<b>1 RPKI Engine Reference Manual</b>	<b>1</b>
<b>2 Further Reading</b>	<b>2</b>
<b>3 Installation Guide</b>	<b>2</b>
<b>4 Configuration Guide</b>	<b>5</b>
<b>5 Operation Guide</b>	<b>9</b>
5.1 Common Options . . . . .	11
5.2 rpkid . . . . .	12
5.3 pubd . . . . .	13
5.4 rootd . . . . .	14
5.5 irdbd . . . . .	15
5.6 irbe_cli . . . . .	16
5.7 cross_certify . . . . .	19
5.8 cronjob . . . . .	19
5.9 smoketest: . . . . .	19
5.10 testpoke . . . . .	22
<b>6 Left-right protocol</b>	<b>23</b>
6.1 Terminology . . . . .	23
6.2 initiated by the IRBE . . . . .	23
6.2.1 <self/> object . . . . .	24
6.2.2 <bsc/> object . . . . .	25
6.2.3 <parent/> object . . . . .	26
6.2.4 <child/> object . . . . .	28
6.2.5 <repository/> object . . . . .	29
6.2.6 <route_origin/> object . . . . .	29
6.3 Operations initiated by the RPKI engine . . . . .	31
6.3.1 <list_resources/> messages . . . . .	31
6.4 Error handling . . . . .	32

<b>7 Publication protocol</b>	<b>32</b>
7.1 Terminology . . . . .	33
7.2 Publication control subprotocol . . . . .	33
7.2.1 <config/> object . . . . .	33
7.2.2 <client/> object . . . . .	34
7.3 Publication subprotocol . . . . .	34
7.3.1 <certificate/> object . . . . .	34
7.3.2 <crl/> object . . . . .	35
7.3.3 <manifest/> object . . . . .	35
7.3.4 <roa/> object . . . . .	35
7.4 Error handling . . . . .	35
7.5 Additional access control considerations. . . . .	36
<b>8 SQL database schemas</b>	<b>37</b>
8.1 rpkid SQL schema . . . . .	39
8.2 pubd SQL Schema . . . . .	44
8.3 irdbd SQL Schema . . . . .	45
<b>9 BPKI model</b>	<b>47</b>
<b>10 Namespace Documentation</b>	<b>50</b>
10.1 Package irbe_cli . . . . .	50
10.1.1 Detailed Description . . . . .	51
10.1.2 Function Documentation . . . . .	52
10.1.3 Variable Documentation . . . . .	52
10.2 Package irdbd . . . . .	54
10.2.1 Detailed Description . . . . .	55
10.2.2 Function Documentation . . . . .	55
10.2.3 Variable Documentation . . . . .	56
10.3 Package pubd . . . . .	58
10.3.1 Detailed Description . . . . .	59
10.3.2 Function Documentation . . . . .	59

10.3.3 Variable Documentation . . . . .	60
10.4 Package rootd . . . . .	60
10.4.1 Detailed Description . . . . .	61
10.4.2 Function Documentation . . . . .	62
10.4.3 Variable Documentation . . . . .	64
10.5 Package rpki . . . . .	68
10.6 Package rpki.__doc__ . . . . .	68
10.7 Package rpki.async . . . . .	68
10.7.1 Detailed Description . . . . .	69
10.7.2 Function Documentation . . . . .	69
10.7.3 Variable Documentation . . . . .	70
10.8 Package rpki.cli . . . . .	71
10.8.1 Detailed Description . . . . .	71
10.8.2 Function Documentation . . . . .	71
10.8.3 Variable Documentation . . . . .	72
10.9 Package rpki.config . . . . .	72
10.9.1 Detailed Description . . . . .	72
10.10 Package rpki.exceptions . . . . .	73
10.10.1 Detailed Description . . . . .	74
10.11 Package rpki.https . . . . .	75
10.11.1 Detailed Description . . . . .	76
10.11.2 Function Documentation . . . . .	77
10.11.3 Variable Documentation . . . . .	78
10.12 Package rpki.ipaddrs . . . . .	80
10.12.1 Detailed Description . . . . .	80
10.13 Package rpki.left_right . . . . .	81
10.13.1 Detailed Description . . . . .	81
10.13.2 Variable Documentation . . . . .	82
10.14 Package rpki.log . . . . .	82
10.14.1 Detailed Description . . . . .	83
10.14.2 Function Documentation . . . . .	83

10.14.3 Variable Documentation . . . . .	84
10.15 Package rpkি.manifest . . . . .	85
10.15.1 Detailed Description . . . . .	86
10.16 Package rpkি.oids . . . . .	86
10.16.1 Detailed Description . . . . .	86
10.16.2 Variable Documentation . . . . .	87
10.17 Package rpkি.publication . . . . .	88
10.17.1 Detailed Description . . . . .	88
10.18 Package rpkি.relaxng . . . . .	89
10.18.1 Variable Documentation . . . . .	89
10.19 Package rpkি.resource_set . . . . .	89
10.19.1 Detailed Description . . . . .	90
10.19.2 Function Documentation . . . . .	91
10.19.3 Variable Documentation . . . . .	92
10.20 Package rpkি.roa . . . . .	92
10.20.1 Detailed Description . . . . .	92
10.21 Package rpkি.rpki_engine . . . . .	93
10.21.1 Detailed Description . . . . .	94
10.22 Package rpkি.sql . . . . .	94
10.22.1 Detailed Description . . . . .	94
10.23 Package rpkি.sundial . . . . .	95
10.23.1 Detailed Description . . . . .	95
10.23.2 Function Documentation . . . . .	96
10.24 Package rpkি.up_down . . . . .	97
10.24.1 Detailed Description . . . . .	97
10.24.2 Variable Documentation . . . . .	98
10.25 Package rpkি.x509 . . . . .	98
10.25.1 Detailed Description . . . . .	99
10.25.2 Function Documentation . . . . .	100
10.26 Package rpkি.xml_utils . . . . .	100
10.26.1 Detailed Description . . . . .	101

10.27 Package rpkid . . . . .	101
10.27.1 Detailed Description . . . . .	101
10.27.2 Function Documentation . . . . .	102
10.27.3 Variable Documentation . . . . .	102
<b>11 Class Documentation</b> . . . . .	<b>103</b>
11.1 <code>async_chat</code> Class Reference . . . . .	103
11.2 <code>dispatcher</code> Class Reference . . . . .	103
11.3 <code>Cmd</code> Class Reference . . . . .	103
11.4 <code>Exception</code> Class Reference . . . . .	103
11.5 <code>irbe_cli.bsc_elt</code> Class Reference . . . . .	103
11.5.1 Detailed Description . . . . .	105
11.5.2 Member Function Documentation . . . . .	105
11.5.3 Member Data Documentation . . . . .	106
11.6 <code>irbe_cli.certificate_elt</code> Class Reference . . . . .	106
11.6.1 Detailed Description . . . . .	107
11.7 <code>irbe_cli.child_elt</code> Class Reference . . . . .	108
11.7.1 Detailed Description . . . . .	110
11.8 <code>irbe_cli.client_elt</code> Class Reference . . . . .	110
11.8.1 Detailed Description . . . . .	112
11.9 <code>irbe_cli.cmd_elt_mixin</code> Class Reference . . . . .	112
11.9.1 Detailed Description . . . . .	114
11.9.2 Member Function Documentation . . . . .	114
11.9.3 Member Data Documentation . . . . .	116
11.10 <code>irbe_cli.cmd_msg_mixin</code> Class Reference . . . . .	117
11.10.1 Detailed Description . . . . .	118
11.10.2 Member Function Documentation . . . . .	118
11.11 <code>irbe_cli.config_elt</code> Class Reference . . . . .	118
11.11.1 Detailed Description . . . . .	120
11.11.2 Member Function Documentation . . . . .	120
11.11.3 Member Data Documentation . . . . .	120

11.12irbe_cli.crl_elt Class Reference . . . . .	120
11.12.1 Detailed Description . . . . .	121
11.13irbe_cli.left_right_cms_msg Class Reference . . . . .	122
11.13.1 Detailed Description . . . . .	123
11.13.2 Member Data Documentation . . . . .	123
11.14irbe_cli.left_right_msg Class Reference . . . . .	123
11.14.1 Detailed Description . . . . .	125
11.14.2 Member Data Documentation . . . . .	125
11.15irbe_cli.left_right_proto Class Reference . . . . .	125
11.15.1 Detailed Description . . . . .	126
11.15.2 Member Data Documentation . . . . .	126
11.16irbe_cli.left_right_sax_handler Class Reference . . . . .	127
11.16.1 Detailed Description . . . . .	128
11.16.2 Member Data Documentation . . . . .	128
11.17irbe_cli.list_published_objects_elt Class Reference . . . . .	128
11.17.1 Detailed Description . . . . .	130
11.17.2 Member Data Documentation . . . . .	130
11.18irbe_cli.list_received_resources_elt Class Reference . . . . .	130
11.18.1 Detailed Description . . . . .	132
11.18.2 Member Data Documentation . . . . .	132
11.19irbe_cli.manifest_elt Class Reference . . . . .	132
11.19.1 Detailed Description . . . . .	133
11.20irbe_cli.parent_elt Class Reference . . . . .	134
11.20.1 Detailed Description . . . . .	136
11.21irbe_cli.publication_cms_msg Class Reference . . . . .	136
11.21.1 Detailed Description . . . . .	137
11.21.2 Member Data Documentation . . . . .	138
11.22irbe_cli.publication_msg Class Reference . . . . .	138
11.22.1 Detailed Description . . . . .	140
11.22.2 Member Data Documentation . . . . .	140
11.23irbe_cli.publication_proto Class Reference . . . . .	140

11.23.1 Detailed Description . . . . .	141
11.23.2 Member Data Documentation . . . . .	141
11.24irbe_cli.publication_sax_handler Class Reference . . . . .	142
11.24.1 Detailed Description . . . . .	143
11.24.2 Member Data Documentation . . . . .	143
11.25irbe_cli.reply_elt_mixin Class Reference . . . . .	143
11.25.1 Detailed Description . . . . .	144
11.25.2 Member Function Documentation . . . . .	144
11.25.3 Member Data Documentation . . . . .	145
11.26irbe_cli.report_error_elt Class Reference . . . . .	145
11.26.1 Detailed Description . . . . .	146
11.27irbe_cli.repository_elt Class Reference . . . . .	146
11.27.1 Detailed Description . . . . .	148
11.28irbe_cli.roa_elt Class Reference . . . . .	148
11.28.1 Detailed Description . . . . .	149
11.29irbe_cli.self_elt Class Reference . . . . .	150
11.29.1 Detailed Description . . . . .	152
11.30irbe_cli.UsageWrapper Class Reference . . . . .	152
11.30.1 Detailed Description . . . . .	152
11.30.2 Member Function Documentation . . . . .	153
11.31long Class Reference . . . . .	153
11.32object Class Reference . . . . .	153
11.33pubd.pubd_context Class Reference . . . . .	153
11.33.1 Detailed Description . . . . .	155
11.33.2 Member Function Documentation . . . . .	155
11.33.3 Member Data Documentation . . . . .	156
11.34datetime Class Reference . . . . .	158
11.35timedelta Class Reference . . . . .	158
11.36rootd.cms_msg Class Reference . . . . .	158
11.36.1 Detailed Description . . . . .	159
11.36.2 Member Data Documentation . . . . .	160

11.37rootd.issue_pdu Class Reference . . . . .	160
11.37.1 Detailed Description . . . . .	161
11.37.2 Member Function Documentation . . . . .	162
11.38rootd.list_pdu Class Reference . . . . .	162
11.38.1 Detailed Description . . . . .	163
11.38.2 Member Function Documentation . . . . .	164
11.39rootd.message_pdu Class Reference . . . . .	164
11.39.1 Detailed Description . . . . .	166
11.39.2 Member Function Documentation . . . . .	166
11.39.3 Member Data Documentation . . . . .	166
11.40rootd.revoke_pdu Class Reference . . . . .	167
11.40.1 Detailed Description . . . . .	168
11.40.2 Member Function Documentation . . . . .	168
11.41rootd.sax_handler Class Reference . . . . .	168
11.41.1 Detailed Description . . . . .	169
11.41.2 Member Data Documentation . . . . .	170
11.42rpki.async.gc_summary Class Reference . . . . .	170
11.42.1 Detailed Description . . . . .	171
11.42.2 Member Function Documentation . . . . .	171
11.42.3 Member Data Documentation . . . . .	171
11.43rpki.async.iterator Class Reference . . . . .	172
11.43.1 Detailed Description . . . . .	173
11.43.2 Member Function Documentation . . . . .	173
11.43.3 Member Data Documentation . . . . .	174
11.44rpki.async.sync_wrapper Class Reference . . . . .	175
11.44.1 Detailed Description . . . . .	177
11.44.2 Member Function Documentation . . . . .	177
11.44.3 Member Data Documentation . . . . .	178
11.45rpki.async.timer Class Reference . . . . .	178
11.45.1 Detailed Description . . . . .	180
11.45.2 Member Function Documentation . . . . .	181

11.45.3 Member Data Documentation . . . . .	183
11.46rpki.cli.Cmd Class Reference . . . . .	184
11.46.1 Detailed Description . . . . .	186
11.46.2 Member Function Documentation . . . . .	186
11.46.3 Member Data Documentation . . . . .	188
11.47rpki.config.parser Class Reference . . . . .	189
11.47.1 Detailed Description . . . . .	191
11.47.2 Member Function Documentation . . . . .	191
11.47.3 Member Data Documentation . . . . .	193
11.48rpki.exceptions.BadClassNameSyntax Class Reference . . . . .	194
11.48.1 Detailed Description . . . . .	195
11.49rpki.exceptions.BadClientURL Class Reference . . . . .	195
11.49.1 Detailed Description . . . . .	196
11.50rpki.exceptions.BadContactURL Class Reference . . . . .	196
11.50.1 Detailed Description . . . . .	197
11.51rpki.exceptions.BadExtension Class Reference . . . . .	197
11.51.1 Detailed Description . . . . .	198
11.52rpki.exceptions.BadIRDBReply Class Reference . . . . .	198
11.52.1 Detailed Description . . . . .	199
11.53rpki.exceptions.BadIssueResponse Class Reference . . . . .	199
11.53.1 Detailed Description . . . . .	200
11.54rpki.exceptions.BadPKCS10 Class Reference . . . . .	200
11.54.1 Detailed Description . . . . .	201
11.55rpki.exceptions.BadPublicationReply Class Reference . . . . .	201
11.55.1 Detailed Description . . . . .	202
11.56rpki.exceptions.BadQuery Class Reference . . . . .	202
11.56.1 Detailed Description . . . . .	203
11.57rpki.exceptions.BadSender Class Reference . . . . .	203
11.57.1 Detailed Description . . . . .	204
11.58rpki.exceptions.BadStatusCode Class Reference . . . . .	204
11.58.1 Detailed Description . . . . .	205

11.59rpki.exceptions.BadURISyntax Class Reference . . . . .	205
11.59.1 Detailed Description . . . . .	206
11.60rpki.exceptions.BSCNotFound Class Reference . . . . .	206
11.60.1 Detailed Description . . . . .	207
11.61rpki.exceptions.BSCNotReady Class Reference . . . . .	207
11.61.1 Detailed Description . . . . .	208
11.62rpki.exceptions.ChildNotFound Class Reference . . . . .	208
11.62.1 Detailed Description . . . . .	209
11.63rpki.exceptions.ClassNameMismatch Class Reference . . . . .	209
11.63.1 Detailed Description . . . . .	210
11.64rpki.exceptions.ClassNameUnknown Class Reference . . . . .	210
11.64.1 Detailed Description . . . . .	211
11.65rpki.exceptions.ClientNotFound Class Reference . . . . .	211
11.65.1 Detailed Description . . . . .	212
11.66rpki.exceptions.CMSSContentNotSet Class Reference . . . . .	212
11.66.1 Detailed Description . . . . .	213
11.67rpki.exceptions.CMSCRLNotSet Class Reference . . . . .	214
11.67.1 Detailed Description . . . . .	214
11.68rpki.exceptions.CMSVerificationFailed Class Reference . . . . .	215
11.68.1 Detailed Description . . . . .	215
11.69rpki.exceptions.DBConsistencyError Class Reference . . . . .	216
11.69.1 Detailed Description . . . . .	216
11.70rpki.exceptions.DEROObjectConversionError Class Reference . . . . .	217
11.70.1 Detailed Description . . . . .	217
11.71rpki.exceptions.DuplicateObject Class Reference . . . . .	218
11.71.1 Detailed Description . . . . .	218
11.72rpki.exceptions.EmptyPEM Class Reference . . . . .	219
11.72.1 Detailed Description . . . . .	219
11.73rpki.exceptions.EmptyROAPrefixList Class Reference . . . . .	220
11.73.1 Detailed Description . . . . .	220
11.74rpki.exceptions.ForbiddenURI Class Reference . . . . .	221

11.74.1 Detailed Description . . . . .	221
11.75rpki.exceptions.HandleTranslationError Class Reference . . . . .	222
11.75.1 Detailed Description . . . . .	222
11.76rpki.exceptions.HTTPRequestFailed Class Reference . . . . .	223
11.76.1 Detailed Description . . . . .	223
11.77rpki.exceptions.HTTPSBadVersion Class Reference . . . . .	224
11.77.1 Detailed Description . . . . .	224
11.78rpki.exceptions.HTTPSClientAborted Class Reference . . . . .	225
11.78.1 Detailed Description . . . . .	225
11.79rpki.exceptions.HTTPSUnexpectedState Class Reference . . . . .	226
11.79.1 Detailed Description . . . . .	226
11.80rpki.exceptions.MissingCMSCRL Class Reference . . . . .	227
11.80.1 Detailed Description . . . . .	227
11.81rpki.exceptions.MissingCMSEcert Class Reference . . . . .	228
11.81.1 Detailed Description . . . . .	228
11.82rpki.exceptions.MultipleTLSEECert Class Reference . . . . .	229
11.82.1 Detailed Description . . . . .	230
11.83rpki.exceptions.MustBePrefix Class Reference . . . . .	230
11.83.1 Detailed Description . . . . .	231
11.84rpki.exceptions.NoActiveCA Class Reference . . . . .	231
11.84.1 Detailed Description . . . . .	232
11.85rpki.exceptions.NoCoveringCertForROA Class Reference . . . . .	232
11.85.1 Detailed Description . . . . .	233
11.86rpki.exceptions.NoObjectAtURI Class Reference . . . . .	233
11.86.1 Detailed Description . . . . .	234
11.87rpki.exceptions.NotACertificateChain Class Reference . . . . .	234
11.87.1 Detailed Description . . . . .	235
11.88rpki.exceptions.NotFound Class Reference . . . . .	235
11.88.1 Detailed Description . . . . .	236
11.89rpki.exceptions.NotImplementedYet Class Reference . . . . .	236
11.89.1 Detailed Description . . . . .	237

11.90rpki.exceptions.NotInDatabase Class Reference . . . . .	237
11.90.1 Detailed Description . . . . .	238
11.91rpki.exceptions.ReceivedTLSCACert Class Reference . . . . .	238
11.91.1 Detailed Description . . . . .	239
11.92rpki.exceptions.RPKI_Exception Class Reference . . . . .	240
11.92.1 Detailed Description . . . . .	241
11.93rpki.exceptions.ServerShuttingDown Class Reference . . . . .	241
11.93.1 Detailed Description . . . . .	242
11.94rpki.exceptions.SKIMismatch Class Reference . . . . .	242
11.94.1 Detailed Description . . . . .	243
11.95rpki.exceptions.SubprocessError Class Reference . . . . .	243
11.95.1 Detailed Description . . . . .	244
11.96rpki.exceptions.TLSValidation Error Class Reference . . . . .	244
11.96.1 Detailed Description . . . . .	245
11.97rpki.exceptions.UnexpectedCMSCerts Class Reference . . . . .	246
11.97.1 Detailed Description . . . . .	246
11.98rpki.exceptions.UnexpectedCMSCRLs Class Reference . . . . .	247
11.98.1 Detailed Description . . . . .	247
11.99rpki.exceptions.UnparsableCMSDER Class Reference . . . . .	248
11.99.1 Detailed Description . . . . .	248
11.100rpki.exceptions.UpstreamError Class Reference . . . . .	249
11.100.1 Detailed Description . . . . .	249
11.101rpki.exceptions.WrongEContentType Class Reference . . . . .	250
11.101.1 Detailed Description . . . . .	250
11.102rpki.https.caller Class Reference . . . . .	251
11.102.1 Detailed Description . . . . .	252
11.102.2 Member Function Documentation . . . . .	252
11.102.3 Member Data Documentation . . . . .	252
11.103rpki.https.http_client Class Reference . . . . .	253
11.103.1 Detailed Description . . . . .	255
11.103.2 Member Function Documentation . . . . .	255

11.103.3Member Data Documentation . . . . .	258
11.104pki.https.http_listener Class Reference . . . . .	260
11.104.1Detailed Description . . . . .	261
11.104.2Member Function Documentation . . . . .	261
11.104.3Member Data Documentation . . . . .	262
11.105pki.https.http_message Class Reference . . . . .	263
11.105.1Detailed Description . . . . .	264
11.105.2Member Function Documentation . . . . .	264
11.105.3Member Data Documentation . . . . .	266
11.106pki.https.http_queue Class Reference . . . . .	266
11.106.1Detailed Description . . . . .	268
11.106.2Member Function Documentation . . . . .	268
11.106.3Member Data Documentation . . . . .	269
11.107pki.https.http_request Class Reference . . . . .	270
11.107.1Detailed Description . . . . .	272
11.107.2Member Function Documentation . . . . .	272
11.107.3Member Data Documentation . . . . .	273
11.108pki.https.http_response Class Reference . . . . .	273
11.108.1Detailed Description . . . . .	275
11.108.2Member Function Documentation . . . . .	275
11.108.3Member Data Documentation . . . . .	275
11.109pki.https.http_server Class Reference . . . . .	276
11.109.1Detailed Description . . . . .	278
11.109.2Member Function Documentation . . . . .	278
11.109.3Member Data Documentation . . . . .	280
11.110pki.https.http_stream Class Reference . . . . .	281
11.110.1Detailed Description . . . . .	283
11.110.2Member Function Documentation . . . . .	284
11.110.3Member Data Documentation . . . . .	289
11.111pki.ipaddrs.v4addr Class Reference . . . . .	290
11.111.1Detailed Description . . . . .	291

11.111.2Member Function Documentation . . . . .	291
11.111.3Member Data Documentation . . . . .	292
11.112pk.i.ipaddrs.v6addr Class Reference . . . . .	292
11.112.1Detailed Description . . . . .	293
11.112.2Member Function Documentation . . . . .	294
11.112.3Member Data Documentation . . . . .	294
11.113pk.i.left_right.bsc_elt Class Reference . . . . .	295
11.113.1Detailed Description . . . . .	297
11.113.2Member Function Documentation . . . . .	297
11.113.3Member Data Documentation . . . . .	298
11.114pk.i.left_right.child_elt Class Reference . . . . .	300
11.114.1Detailed Description . . . . .	302
11.114.2Member Function Documentation . . . . .	302
11.114.3Member Data Documentation . . . . .	304
11.115pk.i.left_right.cms_msg Class Reference . . . . .	305
11.115.1Detailed Description . . . . .	307
11.115.2Member Data Documentation . . . . .	307
11.116pk.i.left_right.data_elt Class Reference . . . . .	307
11.116.1Detailed Description . . . . .	309
11.116.2Member Function Documentation . . . . .	309
11.116.3Member Data Documentation . . . . .	311
11.117pk.i.left_right.left_right_namespace Class Reference . . . . .	311
11.117.1Detailed Description . . . . .	312
11.117.2Member Data Documentation . . . . .	312
11.118pk.i.left_right.list_published_objects_elt Class Reference . . . . .	313
11.118.1Detailed Description . . . . .	315
11.118.2Member Function Documentation . . . . .	315
11.118.3Member Data Documentation . . . . .	316
11.119pk.i.left_right.list_received_resources_elt Class Reference . . . . .	316
11.119.1Detailed Description . . . . .	318
11.119.2Member Function Documentation . . . . .	318

11.119.3Member Data Documentation . . . . .	318
11.120pki.left_right.list_resources_elt Class Reference . . . . .	319
11.120.1Detailed Description . . . . .	321
11.120.2Member Function Documentation . . . . .	321
11.120.3Member Data Documentation . . . . .	322
11.121pki.left_right.list_roa_requests_elt Class Reference . . . . .	323
11.121.1Detailed Description . . . . .	324
11.121.2Member Function Documentation . . . . .	324
11.121.3Member Data Documentation . . . . .	324
11.122pki.left_right.msg Class Reference . . . . .	325
11.122.1Detailed Description . . . . .	327
11.122.2Member Function Documentation . . . . .	327
11.122.3Member Data Documentation . . . . .	327
11.123pki.left_right.parent_elt Class Reference . . . . .	328
11.123.1Detailed Description . . . . .	330
11.123.2Member Function Documentation . . . . .	330
11.123.3Member Data Documentation . . . . .	332
11.124pki.left_right.report_error_elt Class Reference . . . . .	334
11.124.1Detailed Description . . . . .	336
11.124.2Member Function Documentation . . . . .	336
11.124.3Member Data Documentation . . . . .	337
11.125pki.left_right.repository_elt Class Reference . . . . .	338
11.125.1Detailed Description . . . . .	340
11.125.2Member Function Documentation . . . . .	340
11.125.3Member Data Documentation . . . . .	341
11.126pki.left_right.sax_handler Class Reference . . . . .	342
11.126.1Detailed Description . . . . .	344
11.126.2Member Function Documentation . . . . .	344
11.127pki.left_right.self_elt Class Reference . . . . .	344
11.127.1Detailed Description . . . . .	347
11.127.2Member Function Documentation . . . . .	347

11.127.3Member Data Documentation . . . . .	351
11.128pki.log.logger Class Reference . . . . .	353
11.128.1Detailed Description . . . . .	354
11.128.2Member Function Documentation . . . . .	354
11.128.3Member Data Documentation . . . . .	354
11.129pki.manifest.FileAndHash Class Reference . . . . .	355
11.129.1Detailed Description . . . . .	355
11.129.2Member Function Documentation . . . . .	356
11.129.3Member Data Documentation . . . . .	356
11.130pki.manifest.FilesAndHashes Class Reference . . . . .	356
11.130.1Detailed Description . . . . .	357
11.130.2Member Function Documentation . . . . .	357
11.131pki.manifest.Manifest Class Reference . . . . .	358
11.131.1Detailed Description . . . . .	359
11.131.2Member Function Documentation . . . . .	359
11.131.3Member Data Documentation . . . . .	359
11.132pki.publication.certificate_elt Class Reference . . . . .	360
11.132.1Detailed Description . . . . .	362
11.132.2Member Data Documentation . . . . .	362
11.133pki.publication.client_elt Class Reference . . . . .	362
11.133.1Detailed Description . . . . .	364
11.133.2Member Function Documentation . . . . .	364
11.133.3Member Data Documentation . . . . .	365
11.134pki.publication.cms_msg Class Reference . . . . .	367
11.134.1Detailed Description . . . . .	369
11.134.2Member Data Documentation . . . . .	369
11.135pki.publication.config_elt Class Reference . . . . .	369
11.135.1Detailed Description . . . . .	371
11.135.2Member Function Documentation . . . . .	371
11.135.3Member Data Documentation . . . . .	372
11.136pki.publication.control_elt Class Reference . . . . .	373

11.136.1	Detailed Description	376
11.136.2	Member Function Documentation	376
11.137	pki.publication.crl_elt Class Reference	376
11.137.1	Detailed Description	378
11.137.2	Member Data Documentation	378
11.138	pki.publication.manifest_elt Class Reference	378
11.138.1	Detailed Description	380
11.138.2	Member Data Documentation	380
11.139	pki.publication.msg Class Reference	380
11.139.1	Detailed Description	382
11.139.2	Member Function Documentation	382
11.139.3	Member Data Documentation	382
11.140	pki.publication.publication_namespace Class Reference	383
11.140.1	Detailed Description	383
11.140.2	Member Data Documentation	384
11.141	pki.publication.publication_object_elt Class Reference	384
11.141.1	Detailed Description	386
11.141.2	Member Function Documentation	386
11.141.3	Member Data Documentation	388
11.142	pki.publication.report_error_elt Class Reference	389
11.142.1	Detailed Description	391
11.142.2	Member Function Documentation	391
11.142.3	Member Data Documentation	392
11.143	pki.publication.roa_elt Class Reference	393
11.143.1	Detailed Description	395
11.143.2	Member Data Documentation	395
11.144	pki.publication.sax_handler Class Reference	395
11.144.1	Detailed Description	397
11.144.2	Member Data Documentation	397
11.145	pki.resource_set.resource_bag Class Reference	397
11.145.1	Detailed Description	399

11.145.2Member Function Documentation . . . . .	399
11.145.3Member Data Documentation . . . . .	401
11.146 <pki.resource_set.resource_range .="" .<="" class="" reference="" td=""><td>402</td></pki.resource_set.resource_range>	402
11.146.1Detailed Description . . . . .	403
11.146.2Member Function Documentation . . . . .	403
11.146.3Member Data Documentation . . . . .	403
11.147 <pki.resource_set.resource_range_as .="" .<="" class="" reference="" td=""><td>404</td></pki.resource_set.resource_range_as>	404
11.147.1Detailed Description . . . . .	405
11.147.2Member Function Documentation . . . . .	405
11.147.3Member Data Documentation . . . . .	405
11.148 <pki.resource_set.resource_range_ip .="" .<="" class="" reference="" td=""><td>406</td></pki.resource_set.resource_range_ip>	406
11.148.1Detailed Description . . . . .	408
11.148.2Member Function Documentation . . . . .	408
11.149 <pki.resource_set.resource_range_ipv4 .="" .<="" class="" reference="" td=""><td>409</td></pki.resource_set.resource_range_ipv4>	409
11.149.1Detailed Description . . . . .	411
11.149.2Member Function Documentation . . . . .	411
11.150 <pki.resource_set.resource_range_ipv6 .="" .<="" class="" reference="" td=""><td>411</td></pki.resource_set.resource_range_ipv6>	411
11.150.1Detailed Description . . . . .	413
11.150.2Member Function Documentation . . . . .	413
11.151 <pki.resource_set.resource_set .="" .<="" class="" reference="" td=""><td>413</td></pki.resource_set.resource_set>	413
11.151.1Detailed Description . . . . .	415
11.151.2Member Function Documentation . . . . .	415
11.151.3Member Data Documentation . . . . .	417
11.152 <pki.resource_set.resource_set_as .="" .<="" class="" reference="" td=""><td>418</td></pki.resource_set.resource_set_as>	418
11.152.1Detailed Description . . . . .	419
11.152.2Member Function Documentation . . . . .	419
11.152.3Member Data Documentation . . . . .	420
11.153 <pki.resource_set.resource_set_ip .="" .<="" class="" reference="" td=""><td>420</td></pki.resource_set.resource_set_ip>	420
11.153.1Detailed Description . . . . .	422
11.153.2Member Function Documentation . . . . .	422
11.153.3Member Data Documentation . . . . .	423

11.154	pki.resource_set.resource_set_ipv4 Class Reference . . . . .	423
11.154.1	Detailed Description . . . . .	425
11.154.2	Member Data Documentation . . . . .	425
11.155	pki.resource_set.resource_set_ipv6 Class Reference . . . . .	425
11.155.1	Detailed Description . . . . .	427
11.155.2	Member Data Documentation . . . . .	427
11.156	pki.resource_set.roa_prefix Class Reference . . . . .	427
11.156.1	Detailed Description . . . . .	429
11.156.2	Member Function Documentation . . . . .	429
11.156.3	Member Data Documentation . . . . .	430
11.157	pki.resource_set.roa_prefix_ipv4 Class Reference . . . . .	431
11.157.1	Detailed Description . . . . .	433
11.157.2	Member Data Documentation . . . . .	433
11.158	pki.resource_set.roa_prefix_ipv6 Class Reference . . . . .	433
11.158.1	Detailed Description . . . . .	435
11.158.2	Member Data Documentation . . . . .	435
11.159	pki.resource_set.roa_prefix_set Class Reference . . . . .	435
11.159.1	Detailed Description . . . . .	436
11.159.2	Member Function Documentation . . . . .	437
11.160	pki.resource_set.roa_prefix_set_ipv4 Class Reference . . . . .	438
11.160.1	Detailed Description . . . . .	440
11.160.2	Member Data Documentation . . . . .	440
11.161	pki.resource_set.roa_prefix_set_ipv6 Class Reference . . . . .	440
11.161.1	Detailed Description . . . . .	442
11.161.2	Member Data Documentation . . . . .	442
11.162	pki.roa.ROAIPAddress Class Reference . . . . .	442
11.162.1	Detailed Description . . . . .	443
11.162.2	Member Function Documentation . . . . .	443
11.162.3	Member Data Documentation . . . . .	444
11.163	pki.roa.ROAIPAddresses Class Reference . . . . .	444
11.163.1	Detailed Description . . . . .	445

11.163.2Member Function Documentation . . . . .	445
11.164pki.roa.ROAIPAddressFamilies Class Reference . . . . .	445
11.164.1Detailed Description . . . . .	446
11.164.2Member Function Documentation . . . . .	446
11.165pki.roa.ROAIPAddressFamily Class Reference . . . . .	446
11.165.1Detailed Description . . . . .	447
11.165.2Member Function Documentation . . . . .	447
11.165.3Member Data Documentation . . . . .	448
11.166pki.roa.RouteOriginAttestation Class Reference . . . . .	448
11.166.1Detailed Description . . . . .	449
11.166.2Member Function Documentation . . . . .	449
11.166.3Member Data Documentation . . . . .	449
11.167pki.rpki_engine.ca_detail_obj Class Reference . . . . .	450
11.167.1Detailed Description . . . . .	452
11.167.2Member Function Documentation . . . . .	453
11.167.3Member Data Documentation . . . . .	457
11.168pki.rpki_engine.ca_obj Class Reference . . . . .	459
11.168.1Detailed Description . . . . .	461
11.168.2Member Function Documentation . . . . .	461
11.168.3Member Data Documentation . . . . .	465
11.169pki.rpki_engine.child_cert_obj Class Reference . . . . .	466
11.169.1Detailed Description . . . . .	468
11.169.2Member Function Documentation . . . . .	468
11.169.3Member Data Documentation . . . . .	470
11.170pki.rpki_engine.publication_queue Class Reference . . . . .	471
11.170.1Detailed Description . . . . .	473
11.170.2Member Function Documentation . . . . .	473
11.170.3Member Data Documentation . . . . .	474
11.171pki.rpki_engine.revoked_cert_obj Class Reference . . . . .	475
11.171.1Detailed Description . . . . .	476
11.171.2Member Function Documentation . . . . .	476

11.171.3Member Data Documentation . . . . .	477
11.172 <sup>1</sup> pki.rpki_engine.roa_obj Class Reference . . . . .	478
11.172.1Detailed Description . . . . .	480
11.172.2Member Function Documentation . . . . .	480
11.172.3Member Data Documentation . . . . .	483
11.173 <sup>2</sup> pki.rpki_engine.rpkid_context Class Reference . . . . .	485
11.173.1Detailed Description . . . . .	487
11.173.2Member Function Documentation . . . . .	488
11.173.3Member Data Documentation . . . . .	490
11.174 <sup>3</sup> pki.sql.session Class Reference . . . . .	493
11.174.1Detailed Description . . . . .	494
11.174.2Member Function Documentation . . . . .	495
11.174.3Member Data Documentation . . . . .	496
11.175 <sup>4</sup> pki.sql.sql_persistent Class Reference . . . . .	498
11.175.1Detailed Description . . . . .	500
11.175.2Member Function Documentation . . . . .	500
11.175.3Member Data Documentation . . . . .	504
11.176 <sup>5</sup> pki.sql.template Class Reference . . . . .	505
11.176.1Detailed Description . . . . .	507
11.176.2Member Function Documentation . . . . .	507
11.176.3Member Data Documentation . . . . .	507
11.177 <sup>6</sup> pki.sundial.datetime Class Reference . . . . .	508
11.177.1Detailed Description . . . . .	510
11.177.2Member Function Documentation . . . . .	510
11.177.3Member Data Documentation . . . . .	514
11.178 <sup>7</sup> pki.sundial.timedelta Class Reference . . . . .	514
11.178.1Detailed Description . . . . .	516
11.178.2Member Function Documentation . . . . .	517
11.178.3Member Data Documentation . . . . .	519
11.179 <sup>8</sup> pki.up_down.base_elt Class Reference . . . . .	520
11.179.1Detailed Description . . . . .	521

11.179.2Member Function Documentation . . . . .	521
11.180pki.up_down.certificate_elt Class Reference . . . . .	522
11.180.1Detailed Description . . . . .	524
11.180.2Member Function Documentation . . . . .	524
11.180.3Member Data Documentation . . . . .	525
11.181pki.up_down.class_elt Class Reference . . . . .	525
11.181.1Detailed Description . . . . .	527
11.181.2Member Function Documentation . . . . .	527
11.181.3Member Data Documentation . . . . .	528
11.182pki.up_down.class_response_syntax Class Reference . . . . .	530
11.182.1Detailed Description . . . . .	531
11.182.2Member Function Documentation . . . . .	531
11.182.3Member Data Documentation . . . . .	532
11.183pki.up_down.cms_msg Class Reference . . . . .	532
11.183.1Detailed Description . . . . .	534
11.183.2Member Function Documentation . . . . .	534
11.184pki.up_down.error_response_pdu Class Reference . . . . .	534
11.184.1Detailed Description . . . . .	536
11.184.2Member Function Documentation . . . . .	536
11.184.3Member Data Documentation . . . . .	537
11.185pki.up_down.issue_pdu Class Reference . . . . .	538
11.185.1Detailed Description . . . . .	540
11.185.2Member Function Documentation . . . . .	540
11.185.3Member Data Documentation . . . . .	541
11.186pki.up_down.issue_response_pdu Class Reference . . . . .	542
11.186.1Detailed Description . . . . .	543
11.186.2Member Function Documentation . . . . .	544
11.187pki.up_down.list_pdu Class Reference . . . . .	544
11.187.1Detailed Description . . . . .	546
11.187.2Member Function Documentation . . . . .	546
11.188pki.up_down.list_response_pdu Class Reference . . . . .	547

11.188.1Detailed Description . . . . .	547
11.189 <sup>0</sup> pki.up_down.message_pdu Class Reference . . . . .	548
11.189.1Detailed Description . . . . .	550
11.189.2Member Function Documentation . . . . .	550
11.189.3Member Data Documentation . . . . .	552
11.190 <sup>0</sup> pki.up_down.multi_uri Class Reference . . . . .	553
11.190.1Detailed Description . . . . .	554
11.190.2Member Function Documentation . . . . .	554
11.191 <sup>0</sup> pki.up_down.revoke_pdu Class Reference . . . . .	555
11.191.1Detailed Description . . . . .	557
11.191.2Member Function Documentation . . . . .	557
11.191.3Member Data Documentation . . . . .	558
11.192 <sup>0</sup> pki.up_down.revoke_response_pdu Class Reference . . . . .	558
11.192.1Detailed Description . . . . .	559
11.193 <sup>0</sup> pki.up_down.revoke_syntax Class Reference . . . . .	560
11.193.1Detailed Description . . . . .	561
11.193.2Member Function Documentation . . . . .	561
11.193.3Member Data Documentation . . . . .	561
11.194 <sup>0</sup> pki.up_down.sax_handler Class Reference . . . . .	562
11.194.1Detailed Description . . . . .	564
11.194.2Member Data Documentation . . . . .	564
11.195 <sup>0</sup> pki.x509.CMS_object Class Reference . . . . .	564
11.195.1Detailed Description . . . . .	567
11.195.2Member Function Documentation . . . . .	567
11.195.3Member Data Documentation . . . . .	568
11.196 <sup>0</sup> pki.x509.CRL Class Reference . . . . .	571
11.196.1Detailed Description . . . . .	572
11.196.2Member Function Documentation . . . . .	572
11.196.3Member Data Documentation . . . . .	574
11.197 <sup>0</sup> pki.x509.DeadDrop Class Reference . . . . .	575
11.197.1Detailed Description . . . . .	576

11.197.2Member Function Documentation . . . . .	576
11.197.3Member Data Documentation . . . . .	576
11.198pki.x509.DER_CMS_object Class Reference . . . . .	577
11.198.1Detailed Description . . . . .	578
11.198.2Member Function Documentation . . . . .	578
11.198.3Member Data Documentation . . . . .	578
11.199pki.x509.DER_object Class Reference . . . . .	579
11.199.1Detailed Description . . . . .	581
11.199.2Member Function Documentation . . . . .	581
11.199.3Member Data Documentation . . . . .	586
11.200pki.x509.PEM_converter Class Reference . . . . .	587
11.200.1Detailed Description . . . . .	588
11.200.2Member Function Documentation . . . . .	588
11.200.3Member Data Documentation . . . . .	589
11.201pki.x509.PKCS10 Class Reference . . . . .	589
11.201.1Detailed Description . . . . .	591
11.201.2Member Function Documentation . . . . .	591
11.201.3Member Data Documentation . . . . .	592
11.202pki.x509.ROA Class Reference . . . . .	593
11.202.1Detailed Description . . . . .	595
11.202.2Member Function Documentation . . . . .	595
11.202.3Member Data Documentation . . . . .	595
11.203pki.x509.RSA Class Reference . . . . .	596
11.203.1Detailed Description . . . . .	598
11.203.2Member Function Documentation . . . . .	598
11.203.3Member Data Documentation . . . . .	599
11.204pki.x509.RSAPublic Class Reference . . . . .	600
11.204.1Detailed Description . . . . .	602
11.204.2Member Function Documentation . . . . .	602
11.204.3Member Data Documentation . . . . .	603
11.205pki.x509.SignedManifest Class Reference . . . . .	604

11.205.1	Detailed Description	605
11.205.2	Member Function Documentation	605
11.205.3	Member Data Documentation	606
11.206	pki.x509.X509 Class Reference	606
11.206.1	Detailed Description	608
11.206.2	Member Function Documentation	608
11.206.3	Member Data Documentation	611
11.207	pki.x509.XML_CMS_object Class Reference	612
11.207.1	Detailed Description	614
11.207.2	Member Function Documentation	614
11.207.3	Member Data Documentation	616
11.208	pki.xml_utils.base_elt Class Reference	616
11.208.1	Detailed Description	618
11.208.2	Member Function Documentation	618
11.208.3	Member Data Documentation	620
11.209	pki.xml_utils.data_elt Class Reference	621
11.209.1	Detailed Description	623
11.209.2	Member Function Documentation	623
11.210	pki.xml_utils.msg Class Reference	626
11.210.1	Detailed Description	628
11.210.2	Member Function Documentation	628
11.210.3	Member Data Documentation	629
11.211	pki.xml_utils.sax_handler Class Reference	630
11.211.1	Detailed Description	631
11.211.2	Member Function Documentation	631
11.211.3	Member Data Documentation	633
11.212	pki.xml_utils.text_elt Class Reference	634
11.212.1	Detailed Description	635
11.212.2	Member Function Documentation	635
11.212.3	Member Data Documentation	635
11.213	Sequence Class Reference	636

11.21\$quenceOf Class Reference . . . . .	636
11.21TextWrapper Class Reference . . . . .	636
11.21ContentHandler Class Reference . . . . .	636
<b>12 File Documentation</b>	<b>637</b>
12.1 __doc__.py File Reference . . . . .	637
12.1.1 Detailed Description . . . . .	637
12.2 __init__.py File Reference . . . . .	638
12.3 async.py File Reference . . . . .	638
12.4 cli.py File Reference . . . . .	638
12.5 config.py File Reference . . . . .	639
12.6 exceptions.py File Reference . . . . .	639
12.7 https.py File Reference . . . . .	641
12.8 ipaddrs.py File Reference . . . . .	642
12.9 irbe_cli.py File Reference . . . . .	642
12.10irdbd.py File Reference . . . . .	644
12.11left_right.py File Reference . . . . .	644
12.12log.py File Reference . . . . .	645
12.13manifest.py File Reference . . . . .	646
12.14oids.py File Reference . . . . .	646
12.15pubd.py File Reference . . . . .	647
12.16publication.py File Reference . . . . .	647
12.17relaxng.py File Reference . . . . .	648
12.18resource_set.py File Reference . . . . .	648
12.19roa.py File Reference . . . . .	649
12.20rootd.py File Reference . . . . .	649
12.21rpki_engine.py File Reference . . . . .	651
12.22rpkid.py File Reference . . . . .	651
12.23sql.py File Reference . . . . .	652
12.24sundial.py File Reference . . . . .	652
12.25up_down.py File Reference . . . . .	652

12.26x509.py File Reference . . . . .	653
12.27xml_utils.py File Reference . . . . .	654

# 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 [configuration 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

Installation instructions for rpkid et al.

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

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

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

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

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

- If your Python installation does not already include the sources files needed to compile new Python extension modules, you will need to install whatever package does include those source files. The need for and name of this package varies from system to system. On FreeBSD, the base Python interpreter package includes the development sources; on at least some Linux distributions, you have to install a separate "python-devel" package or something similar. If you get compilation errors trying to build the POW code (below) and the error message says something about the file "Python.h" being missing, this is almost certainly your problem.
- <http://codespeak.net/lxml/>, a Pythonic interface to the Gnome LibXML2 libraries. lxml in turn requires the LibXML2 C libraries.

- FreeBSD: /usr/ports/devel/py-lxml
  - Fedora: python-lxml.i386
  - Ubuntu: python-lxml
- <http://sourceforge.net/projects/mysql-python/>, the Python "db" interface to MySQL. MySQLdb in turn requires MySQL client and server. rpkid et al have been tested with MySQL 5.0 and 5.1.
    - FreeBSD: /usr/ports/databases/py-MySQLdb
    - Fedora: MySQL-python.i386
    - Ubuntu: python-mysqldb

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

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

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

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

This should automatically build everything, in the right order, including 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.

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

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

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

- FreeBSD: /usr/ports/textproc/libxslt
- Ubuntu: xsltproc

All tests should be run from the rpkid/ or myrpki/ directories.

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

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

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

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

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

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

- <http://www.doxygen.org/>. Doxygen in turn pulls in several other tools, notably Graphviz, pdfLaTeX, and Ghostscript.
  - FreeBSD: /usr/ports-devel/doxygen
  - Ubuntu: doxygen
- <http://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

Once you've finished with installation, the next thing you should read is the [Configuration Guide](#).

## 4 Configuration Guide

This section describes the configuration file syntax and settings.

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

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

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

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

```
[myrpki]
```

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

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

```
handle = Me
```

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

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

```
roa_csv = roas.csv
prefix_csv = prefixes.csv
```

```

asn_csv           = asns.csv
xml_filename     = myrpki.xml
bpki_resources_directory = bpki/resources
bpki_servers_directory = bpki/servers

```

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

```

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

run_rpkid          = true

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

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

```

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

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

```

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

run_pubd          = false

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

pubd_server_host    = pubd.example.org
pubd_server_port     = 4402

```

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

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

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

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

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

run_rootd                  = false

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

rootd_server_port           = 4401
```

You shouldn't run rootd unless you're the root of an RPKI tree. Who gets to be the root of the public RPKI tree is a political issue outside the scope of this document. For everybody else, the only reason for running rootd (other than test purposes) would be to support certification of private IP addresses and ASNs. The core tools can do this without any problem, but the simplified configuration mechanism does not (yet) make this easy to do.

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

publication_base_directory    = publication/

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

publication_rsync_module      = rpki
```

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

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

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

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

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

shared_sql_username      = rpki
shared_sql_password      = fnord

# If you want different usernames and passwords for the separate SQL
# databases, enter those settings here; the shared_sql_* settings are
# only referenced here, so you can remove them entirely if you're
# setting everything in this block.

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

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

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

These settings control how `rpkid`, `irdbd`, and `pubd` talk to the MySQL server. At minimum, each daemon needs its own database; in the simplest configuration, the username and password can be shared, which is what the macro references in the default

configuration does. If for some reason you need to set different usernames and passwords for different daemons, you can do so by changing the daemon-specific variables.

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

openssl = openssl
```

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

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

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

### Warning

At this point we should have subpages showing configuration details for the various daemons, for people who really want or need to know. We should also have a configuration example for `rsyncd.conf`.

Once you've finished with configuration, the next thing you should read is the [Operation Guide](#).

## 5 Operation Guide

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`: The main RPKI engine daemon.
- `pubd`: The publication engine daemon.
- `rootd`: A separate daemon for handling the root of an RPKI certificate tree. This is essentially a stripped down version of rpkid with no SQL database, no left-right protocol implementation, and only the parent side of the up-down protocol. It's separate because the root is a special case in several ways and it was simpler to keep the special cases out of the main daemon.
- `irdbd`: A sample implementation of an IR database daemon. rpkid calls into this to perform lookups via the left-right protocol.
- `irbe_cli`: A command-line client for the left-right control protocol. Very obscure syntax, badly needs rewriting.
- `smoketest`: A test tool for running a collection of rpkid and irdb instances under common control, driven by a unified test script.
- `yamlttest` : Another test tool which takes the same input format as `smoketest.py`, but with slightly different purpose. `smoketest.py` is intended to support regression tests, while `yamlttest.py` is intended for automated testing of something closer to a real operational environment. There's a fair amount of code duplication between the two, and at some point they will probably be merged into a single program that supports both modes of operation.
- `testpoke`: A simple client for the up-down protocol, mostly compatible with APNIC's `rpk_i_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 `yamlttest` 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, configuring relationships between parents and children and between publication clients and repositories, starting rpkid, pubd, rootd, and irdbd, and using the left-right and publication control protocols to set up rpkid's and pubd's internal state. All other operations should occur either as a result of cron events or as a result of incoming left-right and up-down protocol requests.

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

At present the daemon programs all run in foreground, that is, 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.

## 5.1 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.

## 5.2 rpkid

rpkid is the main RPKI engine daemon. Configuration of rpkid is a two step process: a config file to bootstrap rpkid to the point where it can speak using the [left-right protocol](#), followed by dynamic configuration via the left-right protocol. 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](#) command line interface or by the smoketest 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.

### 5.3 pubd

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

pubd is separate from rpkid for two reasons:

- The hosting model allows entities which choose to run their own copies of rpkid to publish their output under a common publication point. In general, encouraging shared publication services where practical is a good thing for relying parties, as it will speed up rsync 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.
- **bpxi-ta:** Name of file containing master BPKI trust anchor for pubd. All BPKI validation in pubd traces back to this trust anchor.
- **irbe-cert:** Name of file containing BPKI certificate used by IRBE when talking to pubd.
- **pubd-cert:** Name of file containing BPKI certificate used by pubd.

- pubd-key: Name of file containing RSA key corresponding to pubd-cert.
- server-host: Hostname or IP address on which to listen for HTTPS connections. Current default is INADDR\_ANY (IPv4 0.0.0.0); this will need to be hacked to support IPv6 for production.
- server-port: TCP port on which to listen for HTTPS connections.
- publication-base: Path to base of filesystem tree where pubd should store publishable objects. Default is "publication/".

## 5.4 rootd

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:

- bpki-ta: Name of file containing BPKI trust anchor. All BPKI certificate validation in rootd traces back to this trust anchor.
- rootd-bpki-cert: Name of file containing rootd's own BPKI certificate.
- rootd-bpki-key: Name of file containing RSA key corresponding to rootd-bpki-cert.
- rootd-bpki-crl: Name of file containing BPKI CRL that would cover rootd-bpki-cert had it been revoked.
- child-bpki-cert: Name of file containing BPKI certificate for rootd's one and only child (RPKI engine to which rootd issues an RPKI certificate).
- server-host: Hostname or IP address on which to listen for HTTPS connections. Default is localhost.
- server-port: TCP port on which to listen for HTTPS connections.

- `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 roottd should write RPKI subject certificate, manifest, and CRL.
- `rpkি-subject-cert`: Name of file that roottd should use to save the one and only certificate it issues. Default is "Subroot.cer".
- `rpkি-root-crl`: Name of file to which roottd should save its RPKI CRL. Default is "Root.crl".
- `rpkি-root-manifest`: Name of file to which roottd should save its RPKI manifest. Default is "Root.mnf".
- `rpkি-subject-pkcs10`: Name of file that roottd should use when saving a copy of the received PKCS #10 request for a resource certificate. This is only used for debugging. Default is not to save the PKCS #10 request.

## 5.5 irdbd

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.
- `bpki-ta`: Name of file containing BPKI trust anchor. All BPKI certificate validation in irdbd traces back to this trust anchor.
- `irdbd-cert`: Name of file containing irdbd's own BPKI certificate.
- `irdbd-key`: Name of file containing RSA key corresponding to irdbd-cert.
- `rpkid-cert`: Name of file containing certificate used the one and only by rpkid instance authorized to contact this irdbd instance.
- `https-url`: Service URL for irdbd. Must be a https:// URL.

## 5.6 irbe\_cli

`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 rpkid 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 com-

mands.

--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.

## 5.7 cross\_certify

cross\_certify 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 ]
```

## 5.8 cronjob

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'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.

## 5.9 smoketest:

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

Unlike the programs described above, smoketest takes two configuration files in different languages. The first configuration file uses the same syntax as the above configuration files but is completely optional. The second configuration file is

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

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 smoketest.conf, run smoketest with "-c filename" to change it.

smoketest.conf options:

- `smoketest_dir`: Working directory into which smoketest should write the (many) files it generates. Default is "smoketest.dir".
- `irdb_db_pass`: MySQL password for the "irdb" user. Default is "fnord". You may want to override this.
- `rpkı_db_pass`: MySQL password for the "rpkı" 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 smoketest learns how to run rcynic itself as part of the test suite.

The second configuration file is named smoketest.yaml by default, run smoketest with "-y filename" to change it. The YAML file contains multiple YAML "documents". The first document describes the initial test layout and resource allocations, subsequent documents describe modifications to the initial allocations and other parameters. Resources listed in the initial layout are aggregated automatically, so that a node in the resource hierarchy automatically receives the resources it needs to issue whatever its children are listed as holding. Actions in the subsequent documents are modifications to the current resource set, modifications to validity dates or other non-resource parameters, or special commands like "sleep". 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 "LIR0", 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 smoketest 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".

## 5.10 testpoke

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 rpk\_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 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

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.

## 6 Left-right protocol

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

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

### 6.1 Terminology

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

### 6.2 initiated by the IRBE

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

Fields can be set in either "create" or "set" operations, the difference just being whether the object already exists. A "get" operation returns all visible fields of the object. A

"list" operation returns a list containing what "get" would have returned on each of those objects.

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

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

### 6.2.1 <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.

- `bpk_i_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 `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 per-engine `bpk_i_ta` certificate.
- `bpk_i_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 `bpk_i_glue` certificate should be the issuer of the `bpk_i_cert` certificate and should be issued by the per-engine `bpk_i_ta` certificate; if not needed, the `bpk_i_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.

### 6.2.2 `<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.

### 6.2.3 `<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.

#### 6.2.4 `<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.

### 6.2.5 <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.

### 6.2.6 <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".

## 6.3 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.

### 6.3.1 <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.

## 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 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.

## 7 Publication protocol

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

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

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

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

## 7.1 Terminology

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

## 7.2 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.

### 7.2.1 <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:

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

### 7.2.2 <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.
- **bpki\_cert** (element): BPKI CA certificate for this <client/>. This is used as part of the certificate chain when validating incoming TLS and CMS messages. If the bpki\_glue certificate is in use (below), the bpki\_cert certificate should be issued by the bpki\_glue certificate; otherwise, the bpki\_cert certificate should be issued by the publication engine's bpki\_ta certificate.
- **bpki\_glue** (element): Another BPKI CA certificate for this <client/>, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the bpki\_glue certificate should be the issuer of the bpki\_cert certificate and should be issued by the publication engine's bpki\_ta certificate; if not needed, the bpki\_glue certificate should be left unset.

## 7.3 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.

### 7.3.1 <certificate/> object

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

### 7.3.2 <crl/> object

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

### 7.3.3 <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.

### 7.3.4 <roa/> object

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

## 7.4 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.

## 7.5 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.

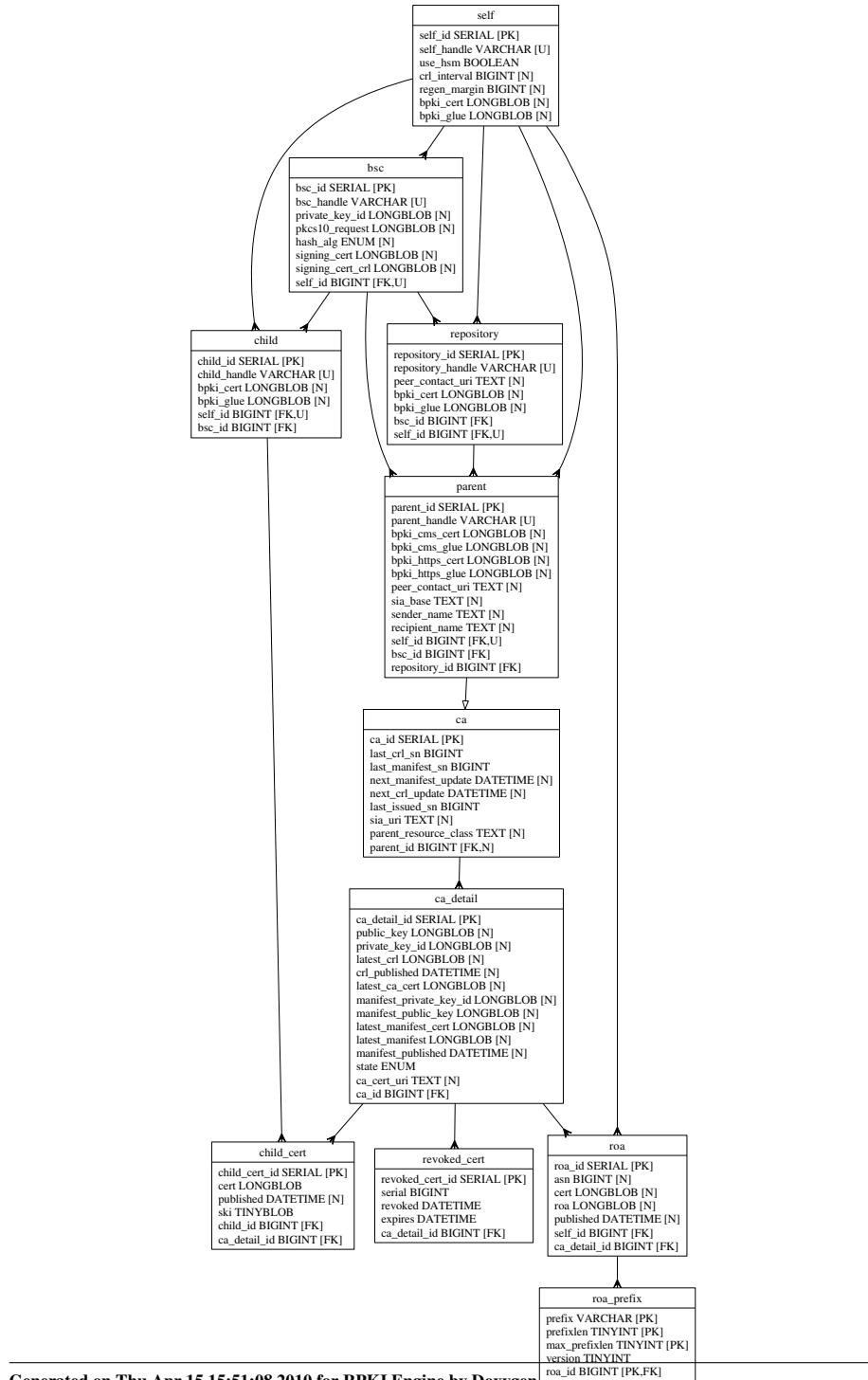
Note that, in this publication model, any agreement that the repository makes to publish the RPKI engine's output is conditional upon the object to be published passing whatever access control checks the publication server imposes.

## 8 SQL database schemas

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



## 8.1 rpkid SQL schema



Generated on Thu Apr 15 15:51:08 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,
    FOREIGN KEY      (self_id, repository_handle)
    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        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,
    FOREIGN KEY        (self_id, parent_handle)
    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,
    bpkı_cert      LONGBLOB,
    bpkı_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:
```

## 8.2 pubd SQL Schema

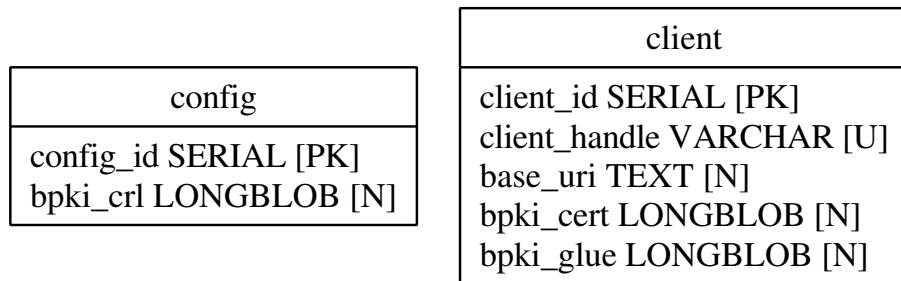


Figure 2: Diagram of pubd.sql

```

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

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

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

-- SQL objects needed by pubd.py.

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

DROP TABLE IF EXISTS client;

```

```

DROP TABLE IF EXISTS config;

CREATE TABLE config (
    config_id      SERIAL NOT NULL,
    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:

```

### 8.3 irdbd SQL Schema

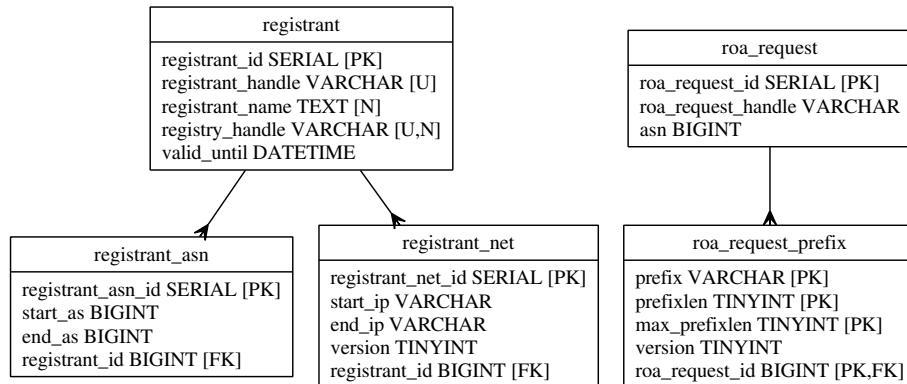


Figure 3: Diagram of irdbd.sql

```

-- $Id: irdbd.sql 2953 2010-01-15 02:50:16Z sra $
-- Copyright (C) 2009-2010 Internet Systems Consortium ("ISC")
--
-- Permission to use, copy, modify, and distribute this software for any
-- purpose with or without fee is hereby granted, provided that the above
-- copyright notice and this permission notice appear in all copies.
--
-- THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH
-- REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY

```

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

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

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

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

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

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

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

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

```

## 9 BPKI model

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

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

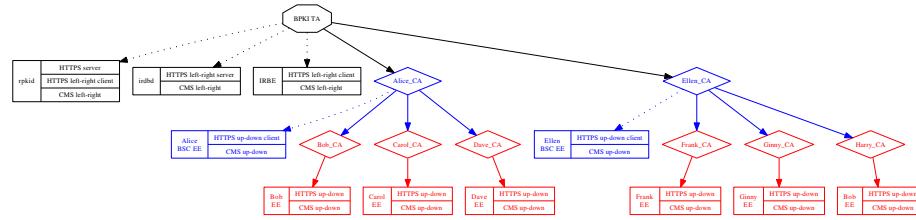
There are a few design principals that underly the chosen BPKI model:

- 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.

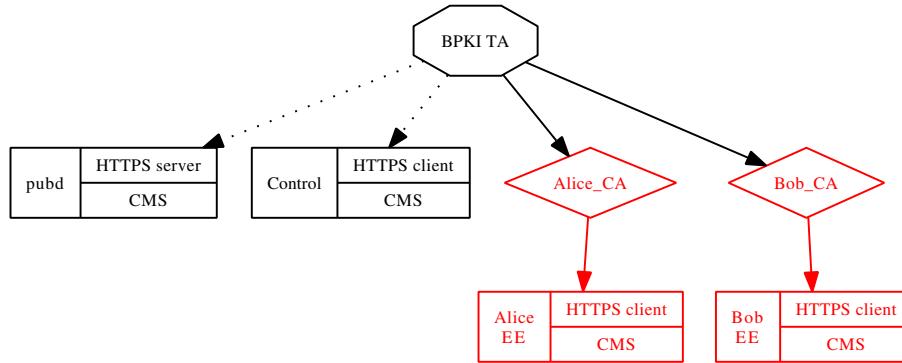
The certificate tree looks complicated, but the set of certificates needed to build any particular validation chain is obvious, again excepting the HTTPS server case, where the client certificate is the first hint that the engine has of the client's identity, so the server must be prepared to accept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

## 10 Namespace Documentation

### 10.1 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_rpkiid`
- 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

### 10.1.1 Detailed Description

Command line IR back-end control program for rpkiid 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.

### 10.1.2 Function Documentation

#### 10.1.2.1 def irbe\_cli.usage ( *code* = 1)

Definition at line 240 of file irbe\_cli.py.

### 10.1.3 Variable Documentation

#### 10.1.3.1 tuple irbe\_cli::argv = sys.argv[1:]

Definition at line 259 of file irbe\_cli.py.

#### 10.1.3.2 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.

#### 10.1.3.3 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.

**10.1.3.4 tuple irbe\_cli.cfg = rpki.config.parser(cfg\_file, "irbe\_cli")**

Definition at line 283 of file irbe\_cli.py.

**10.1.3.5 irbe\_cli.cfg\_file = "irbe.conf"**

Definition at line 264 of file irbe\_cli.py.

**10.1.3.6 irbe\_cli.pem\_out = None**

Definition at line 39 of file irbe\_cli.py.

**10.1.3.7 irbe\_cli.q\_msg = q\_msg\_left\_right**

Definition at line 291 of file irbe\_cli.py.

**10.1.3.8 list irbe\_cli.q\_msg\_left\_right = [ ]**

Definition at line 285 of file irbe\_cli.py.

**10.1.3.9 list irbe\_cli.q\_msg\_publication = [ ]**

Definition at line 286 of file irbe\_cli.py.

**10.1.3.10 list irbe\_cli::q\_pdu = left\_right\_msg.pdus[argv[0]]**

Definition at line 290 of file irbe\_cli.py.

**10.1.3.11 list irbe\_cli.top\_opts = ["config=", "help", "pem\_out=", "quiet", "verbose"]**

Definition at line 238 of file irbe\_cli.py.

**10.1.3.12 tuple irbe\_cli.usage\_fill = UsageWrapper(subsequent\_indent = " " \* 4)**

Definition at line 50 of file irbe\_cli.py.

**10.1.3.13 irbe\_cli.verbose = True**

Definition at line 265 of file irbe\_cli.py.

## 10.2 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"))`

### 10.2.1 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.

### 10.2.2 Function Documentation

#### 10.2.2.1 def irdbd.handle\_list\_resources ( *q\_pdu*, *r\_msg*)

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

**10.2.2.2 def irdbd.handle\_list\_roa\_requests ( *q\_pdu*, *r\_msg* )**

Definition at line 90 of file irdbd.py.

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

Definition at line 119 of file irdbd.py.

**10.2.3 Variable Documentation****10.2.3.1 tuple irdbd.bpk\_i\_ta = rpki.x509.X509(Auto\_file = cfg.get("bpki-ta"))**

Definition at line 201 of file irdbd.py.

**10.2.3.2 tuple irdbd.cfg = rpki.config.parser(cfg\_file, "irdbd")**

Definition at line 186 of file irdbd.py.

**10.2.3.3 irdbd.cfg\_file = "irdbd.conf"**

Definition at line 170 of file irdbd.py.

**10.2.3.4 tuple irdbd.client\_ta = (bpki\_ta, rpkid\_cert)**

Definition at line 217 of file irdbd.py.

**10.2.3.5 tuple irdbd.cur = db.cursor()**

Definition at line 198 of file irdbd.py.

**10.2.3.6 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.

**10.2.3.7 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.

**10.2.3.8 tuple irdbd.handlers = ((u.path, handler),)**

Definition at line 220 of file irdbd.py.

**10.2.3.9 string irdbd.host = "localhost"**

Definition at line 218 of file irdbd.py.

**10.2.3.10 tuple irdbd.irdbd\_cert = rpki.x509.X509(Auto\_file =
cfg.get("irdbd-cert"))**

Definition at line 203 of file irdbd.py.

**10.2.3.11 tuple irdbd.irdbd\_key = rpki.x509.RSA( Auto\_file =
cfg.get("irdbd-key"))**

Definition at line 204 of file irdbd.py.

**10.2.3.12 int irdbd.port = 443**

Definition at line 219 of file irdbd.py.

**10.2.3.13 tuple irdbd.rpkid\_cert = rpki.x509.X509(Auto\_file =  
cfg.get("rpkid-cert"))**

Definition at line 202 of file irdbd.py.

**10.2.3.14 irdbd.server\_cert = irdbd\_cert,**

Definition at line 216 of file irdbd.py.

**10.2.3.15 tuple irdbd.startup\_msg = cfg.get("startup-message", "")**

Definition at line 188 of file irdbd.py.

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

Definition at line 206 of file irdbd.py.

## 10.3 Package pubd

### Classes

- class [pubd\\_context](#)

### Functions

- def [main](#)

## Variables

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

### 10.3.1 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.

### 10.3.2 Function Documentation

#### 10.3.2.1 def pubd.main ()

Definition at line 174 of file pubd.py.

### 10.3.3 Variable Documentation

#### 10.3.3.1 pubd.cfg\_file = "pubd.conf"

Definition at line 155 of file pubd.py.

#### 10.3.3.2 pubd.profile = False

Definition at line 156 of file pubd.py.

## 10.4 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 `rotd_bpki_cert = rpki.x509.X509`(`Auto_file = cfg.get("rotd-bpki-cert")`)
- tuple `rotd_bpki_crl = rpki.x509.CRL`(`Auto_file = cfg.get("rotd-bpki-crl")`)
- tuple `rotd_bpki_key = rpki.x509.RSA`(`Auto_file = cfg.get("rotd-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 = rotd_bpki_cert`,

### 10.4.1 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 rotd.py [ { -c | --config } configfile ] [ { -h | --help } ]
```

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

```
$Id: rotd.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.

### 10.4.2 Function Documentation

#### 10.4.2.1 def roottd.compose\_response (*r\_msg, pkcs10 = None*)

Definition at line 175 of file roottd.py.

#### 10.4.2.2 def roottd.del\_subject\_cert ()

Definition at line 72 of file roottd.py.

#### 10.4.2.3 def roottd.del\_subject\_pkcs10 ()

Definition at line 91 of file roottd.py.

**10.4.2.4 def rootd.get\_root\_cert ()**

Definition at line 48 of file rootd.py.

**10.4.2.5 def rootd.get\_subject\_cert ()**

Definition at line 56 of file rootd.py.

**10.4.2.6 def rootd.get\_subject\_pkcs10 ()**

Definition at line 77 of file rootd.py.

**10.4.2.7 def rootd.issue\_subject\_cert\_maybe ( new\_pkcs10 )**

Definition at line 98 of file rootd.py.

**10.4.2.8 def rootd.root\_newer\_than\_subject ()**

Definition at line 53 of file rootd.py.

**10.4.2.9 def rootd.set\_subject\_cert ( cert )**

Definition at line 65 of file rootd.py.

**10.4.2.10 def rootd.set\_subject\_pkcs10 ( pkcs10 )**

Definition at line 85 of file rootd.py.

**10.4.2.11 def rootd.up\_down\_handler (query, path, cb)**

Definition at line 238 of file rootd.py.

**10.4.3 Variable Documentation****10.4.3.1 tuple rootd.bpki\_ta = rpki.x509.X509(Auto\_file = cfg.get("bpki-ta"))**

Definition at line 288 of file rootd.py.

**10.4.3.2 tuple rootd.cfg = rpki.config.parser(cfg\_file, "rootd")**

Definition at line 284 of file rootd.py.

**10.4.3.3 rootd.cfg\_file = "rootd.conf"**

Definition at line 268 of file rootd.py.

**10.4.3.4 tuple rootd.child\_bpki\_cert = rpki.x509.X509(Auto\_file = cfg.get("child-bpki-cert"))**

Definition at line 292 of file rootd.py.

**10.4.3.5 tuple rootd.client\_ta = (bpki\_ta, child\_bpki\_cert)**

Definition at line 316 of file rootd.py.

**10.4.3.6 rootd.handlers = up\_down\_handler)**

Definition at line 319 of file rootd.py.

**10.4.3.7 rotd.host = https\_server\_host,**

Definition at line 317 of file rotd.py.

**10.4.3.8 tuple rotd.https\_server\_host = cfg.get("server-host", "")**

Definition at line 294 of file rotd.py.

**10.4.3.9 tuple rotd.https\_server\_port = int(cfg.get("server-port"))**

Definition at line 295 of file rotd.py.

**10.4.3.10 rotd.port = https\_server\_port,**

Definition at line 318 of file rotd.py.

**10.4.3.11 tuple rotd.rootd\_bpki\_cert = rpki.x509.X509(Auto\_file =  
cfg.get("rootd-bpki-cert"))**

Definition at line 290 of file rotd.py.

**10.4.3.12 tuple rotd.rootd\_bpki\_crl = rpki.x509.CRL( Auto\_file =  
cfg.get("rootd-bpki-crl"))**

Definition at line 291 of file rotd.py.

**10.4.3.13 tuple rotd.rootd\_bpki\_key = rpki.x509.RSA( Auto\_file =  
cfg.get("rootd-bpki-key"))**

Definition at line 289 of file rotd.py.

**10.4.3.14 tuple roottd.rpki\_base\_uri = cfg.get("rpki-base-uri", "rsync://" + rpki\_class\_name + ".invalid/")**

Definition at line 300 of file roottd.py.

**10.4.3.15 tuple roottd.rpki\_class\_name = cfg.get("rpki-class-name", "wombat")**

Definition at line 297 of file roottd.py.

**10.4.3.16 roottd.rpki\_root\_cert = None**

Definition at line 46 of file roottd.py.

**10.4.3.17 tuple roottd.rpki\_root\_cert\_file = cfg.get("rpki-root-cert")**

Definition at line 303 of file roottd.py.

**10.4.3.18 tuple roottd.rpki\_root\_cert\_uri = cfg.get("rpki-root-cert-uri", rpki\_base\_uri + "Root.cer")**

Definition at line 304 of file roottd.py.

**10.4.3.19 tuple roottd.rpki\_root\_crl = cfg.get("rpki-root-crl", "Root.crl")**

Definition at line 307 of file roottd.py.

**10.4.3.20 tuple roottd.rpki\_root\_dir = cfg.get("rpki-root-dir")**

Definition at line 299 of file roottd.py.

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

Definition at line 302 of file roott.py.

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

Definition at line 306 of file roott.py.

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

Definition at line 308 of file roott.py.

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

Definition at line 311 of file roott.py.

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

Definition at line 309 of file roott.py.

```
10.4.3.26 tuple roott.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 roott.py.

**10.4.3.27 rootd.server\_cert = rootd\_bpki\_cert,**

Definition at line 315 of file rootd.py.

**10.5 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](#)

**10.6 Package rpki.\_\_doc\_\_****10.7 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`

### 10.7.1 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.

### 10.7.2 Function Documentation

#### 10.7.2.1 def rpki.async.\_raiseExitNow (*signum, frame*) [private]

Signal handler for `event_loop()`.

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

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

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

Definition at line 250 of file async.py.

**10.7.2.3 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.

**10.7.2.4 def rpki.async.exit\_event\_loop ()**

Force exit from `event_loop()`.

Definition at line 364 of file async.py.

**10.7.2.5 def rpki.async.run\_deferred ()**

Run deferred actions.

Definition at line 256 of file async.py.

**10.7.3 Variable Documentation****10.7.3.1 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.

### 10.7.3.2 rpki::async.ExitNow = asynccore.ExitNow

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

## 10.8 Package rpki.cli

### Classes

- class [Cmd](#)

### Functions

- def [yes\\_or\\_no](#)

### Variables

- dictionary [\\_yes\\_or\\_no\\_prompts](#)
- [have\\_readline](#) = True

#### 10.8.1 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.

#### 10.8.2 Function Documentation

##### 10.8.2.1 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.

### 10.8.3 Variable Documentation

#### 10.8.3.1 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.

#### 10.8.3.2 rpki::cli.have\_readline = True

Definition at line 25 of file cli.py.

## 10.9 Package rpki.config

### Classes

- class [parser](#)

#### 10.9.1 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.

## 10.10 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](#)

### 10.10.1 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.

## 10.11 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.*

### 10.11.1 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.

### 10.11.2 Function Documentation

#### 10.11.2.1 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.

#### 10.11.2.2 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.

#### 10.11.2.3 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.

#### 10.11.2.4 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.

### 10.11.3 Variable Documentation

#### 10.11.3.1 `rpki::https::client_queues = {}`

Map of (host, port) tuples to [http\\_queue](#) objects.

Definition at line 1032 of file https.py.

#### 10.11.3.2 `rpki::https::debug_http = False`

Verbose chatter about HTTP streams.

Definition at line 45 of file https.py.

#### 10.11.3.3 `rpki::https::debug_tls_certs = False`

Verbose chatter about TLS certificates.

Definition at line 49 of file https.py.

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

Default HTTP client connection timeout.

Definition at line 61 of file https.py.

#### 10.11.3.5 `rpki::https::default_http_version = (1, 0)`

Preferred HTTP version.

Definition at line 72 of file https.py.

**10.11.3.6 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.

**10.11.3.7 rpki::https::rpki\_content\_type = "application/x-rpki"**

HTTP content type used for all RPKI messages.

Definition at line 41 of file https.py.

**10.11.3.8 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.

**10.11.3.9 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.

**10.11.3.10 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.

## 10.12 Package rpki.ipaddrs

### Classes

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

#### 10.12.1 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.

## 10.13 Package rpki.left\_right

### Classes

- class [bsc\\_elt](#)
- class [child\\_elt](#)
- class [cms\\_msg](#)
- class [data\\_elt](#)
- class [left\\_right\\_namespace](#)
- class [list\\_published\\_objects\\_elt](#)
- class [list\\_received\\_resources\\_elt](#)
- class [list\\_resources\\_elt](#)
- class [list\\_roa\\_requests\\_elt](#)
- class [msg](#)
- class [parent\\_elt](#)
- class [report\\_error\\_elt](#)
- class [repository\\_elt](#)
- class [sax\\_handler](#)
- class [self\\_elt](#)

### Variables

- [enforce\\_strict\\_up\\_down\\_xml\\_sender](#) = False

#### 10.13.1 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.

### 10.13.2 Variable Documentation

#### 10.13.2.1 rpki::left\_right.enforce\_strict\_up\_down\_xml\_sender = False

Definition at line 40 of file left\_right.py.

## 10.14 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)

### 10.14.1 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.
```

### 10.14.2 Function Documentation

#### 10.14.2.1 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.

**10.14.2.2 def rpki.log.set\_trace (*enable*)**

Enable or disable call tracing.

Definition at line 63 of file log.py.

**10.14.2.3 def rpki.log.trace ()**

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

Definition at line 91 of file log.py.

**10.14.2.4 def rpki.log.traceback ()**

Consolidated backtrace facility with a bit of extra info.

Definition at line 100 of file log.py.

**10.14.3 Variable Documentation****10.14.3.1 tuple rpki::log.debug = logger(syslog.LOG\_DEBUG)**

Definition at line 89 of file log.py.

**10.14.3.2 rpki::log::enable\_trace = False**

Whether call tracing is enabled.

Definition at line 41 of file log.py.

**10.14.3.3 tuple rpki::log.error = logger(syslog.LOG\_ERR)**

Definition at line 85 of file log.py.

**10.14.3.4 tuple rpki::log.info = logger(syslog.LOG\_INFO)**

Definition at line 88 of file log.py.

**10.14.3.5 tuple rpki::log.note = logger(syslog.LOG\_NOTICE)**

Definition at line 87 of file log.py.

**10.14.3.6 int rpki::log.pid = 0**

Definition at line 49 of file log.py.

**10.14.3.7 string rpki::log.tag = ""**

Definition at line 48 of file log.py.

**10.14.3.8 rpki::log::use\_syslog = True**

Whether to use syslog.

Definition at line 46 of file log.py.

**10.14.3.9 tuple rpki::log.warn = logger(syslog.LOG\_WARNING)**

Definition at line 86 of file log.py.

## 10.15 Package rpki.manifest

### Classes

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

### 10.15.1 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.

## 10.16 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.*

### 10.16.1 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.

### 10.16.2 Variable Documentation

#### 10.16.2.1 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.

#### 10.16.2.2 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.

## 10.17 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](#)

### 10.17.1 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.

## 10.18 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.*

#### 10.18.1 Variable Documentation

##### 10.18.1.1 [rpki::relaxng::left\\_right](#)

Parsed RelaxNG `left_right` schema.

Definition at line 7 of file relaxng.py.

##### 10.18.1.2 [rpki::relaxng::publication](#)

Parsed RelaxNG publication schema.

Definition at line 1252 of file relaxng.py.

##### 10.18.1.3 [rpki::relaxng::up\\_down](#)

Parsed RelaxNG `up_down` schema.

Definition at line 998 of file relaxng.py.

## 10.19 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.*

#### 10.19.1 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.

## 10.19.2 Function Documentation

### 10.19.2.1 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.

### 10.19.2.2 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.

**10.19.2.3 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.

**10.19.2.4 def rpki.resource\_set.test1 (*t, s1, s2*)**

Definition at line 884 of file resource\_set.py.

**10.19.2.5 def rpki.resource\_set.test2 (*t, s1, s2*)**

Definition at line 917 of file resource\_set.py.

**10.19.3 Variable Documentation****10.19.3.1 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.

**10.20 Package rpki.roa****Classes**

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

**10.20.1 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
```

## 10.21 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](#)

### 10.21.1 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.

## 10.22 Package rpki.sql

### Classes

- class [session](#)
- class [sql\\_persistent](#)
- class [template](#)

### 10.22.1 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.

## 10.23 Package rpki.sundial

### Classes

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

### Functions

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

#### 10.23.1 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.
```

### 10.23.2 Function Documentation

#### 10.23.2.1 def rpki.sundial.\_cast (x) [private]

Cast result of arithmetic operations back into correct subtype.

Definition at line 257 of file sundial.py.

#### 10.23.2.2 def rpki.sundial.now ()

Get current timestamp.

Definition at line 50 of file sundial.py.

### 10.23.2.3 def rpki.sundial.test ( t )

Definition at line 269 of file sundial.py.

## 10.24 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/"

### 10.24.1 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.

### 10.24.2 Variable Documentation

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

Definition at line 41 of file up\_down.py.

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

Definition at line 39 of file up\_down.py.

## 10.25 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

### 10.25.1 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.

### 10.25.2 Function Documentation

#### 10.25.2.1 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.

#### 10.25.2.2 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.

#### 10.25.2.3 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.

## 10.26 Package rpki.xml\_utils

### Classes

- class [base\\_elt](#)
- class [data\\_elt](#)
- class [msg](#)
- class [sax\\_handler](#)
- class [text\\_elt](#)

### 10.26.1 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.

## 10.27 Package rpkid

### Functions

- def [main](#)

### Variables

- string [cfg\\_file](#) = "rpkid.conf"
- [profile](#) = None

### 10.27.1 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.
```

## 10.27.2 Function Documentation

### 10.27.2.1 def rpkid.main ()

Definition at line 68 of file rpkid.py.

## 10.27.3 Variable Documentation

### 10.27.3.1 rpkid.cfg\_file = "rpkid.conf"

Definition at line 49 of file rpkid.py.

### 10.27.3.2 rpkid.profile = None

Definition at line 50 of file rpkid.py.

## 11 Class Documentation

### 11.1 async\_chat Class Reference

Inherited by [rpki.https.http\\_stream](#).

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

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

### 11.2 dispatcher Class Reference

Inherited by [rpki.https.http\\_listener](#).

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

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

### 11.3 Cmd Class Reference

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

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

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

### 11.4 Exception Class Reference

Inherited by [rpki.exceptions.RPKI\\_Exception](#).

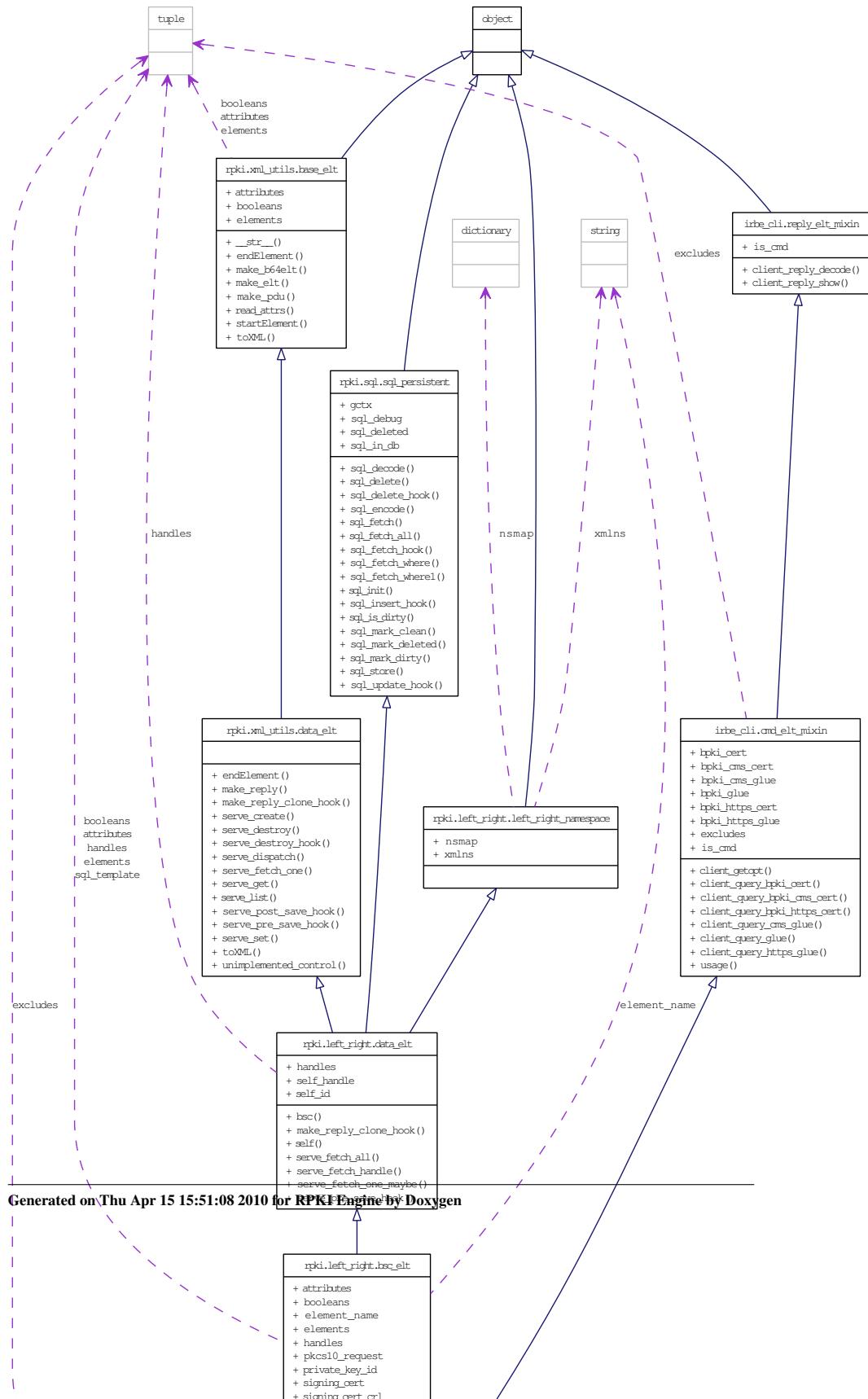
The documentation for this class was generated from the following file:

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

### 11.5 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.*

#### 11.5.1 Detailed Description

Definition at line 152 of file irbe\_cli.py.

#### 11.5.2 Member Function Documentation

##### 11.5.2.1 def `irbe_cli.bsc_elt.client_query_signing_cert (self, arg)`

--signing\_cert option.

Definition at line 156 of file irbe\_cli.py.

##### 11.5.2.2 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.

**11.5.2.3 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](#).

**11.5.3 Member Data Documentation****11.5.3.1 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](#).

**11.5.3.2 irbe\_cli.bsc\_elt.signing\_cert**

Reimplemented from [rpki.left\\_right.bsc\\_elt](#).

Definition at line 158 of file [irbe\\_cli.py](#).

**11.5.3.3 irbe\_cli.bsc\_elt.signing\_cert\_crl**

Reimplemented from [rpki.left\\_right.bsc\\_elt](#).

Definition at line 162 of file [irbe\\_cli.py](#).

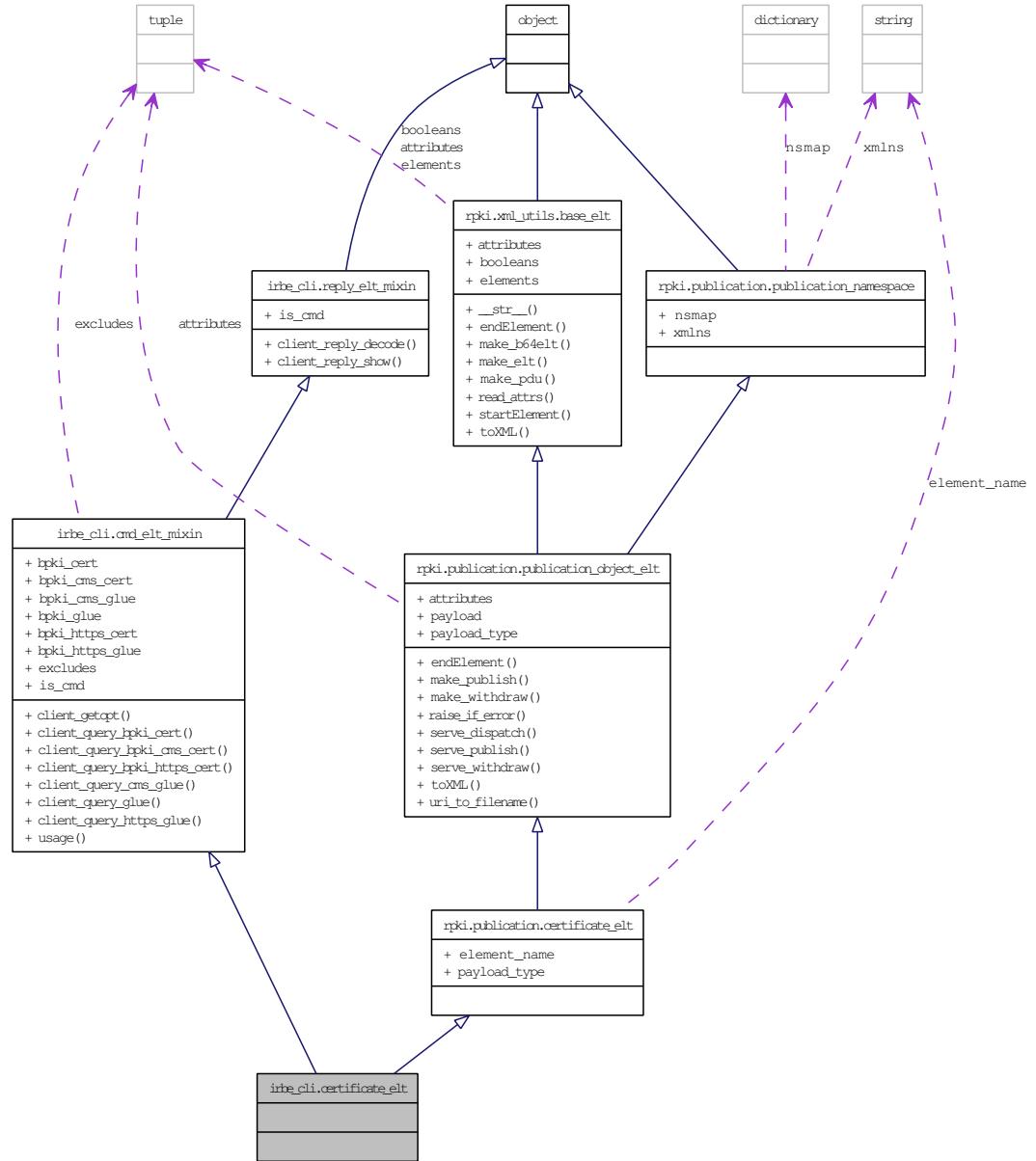
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

**11.6 irbe\_cli.certificate\_elt Class Reference**

Inherits [irbe\\_cli::cmd\\_elt\\_mixin](#), and [rpki::publication::certificate\\_elt](#).

Collaboration diagram for irbe\_cli.certificate\_elt:



### 11.6.1 Detailed Description

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

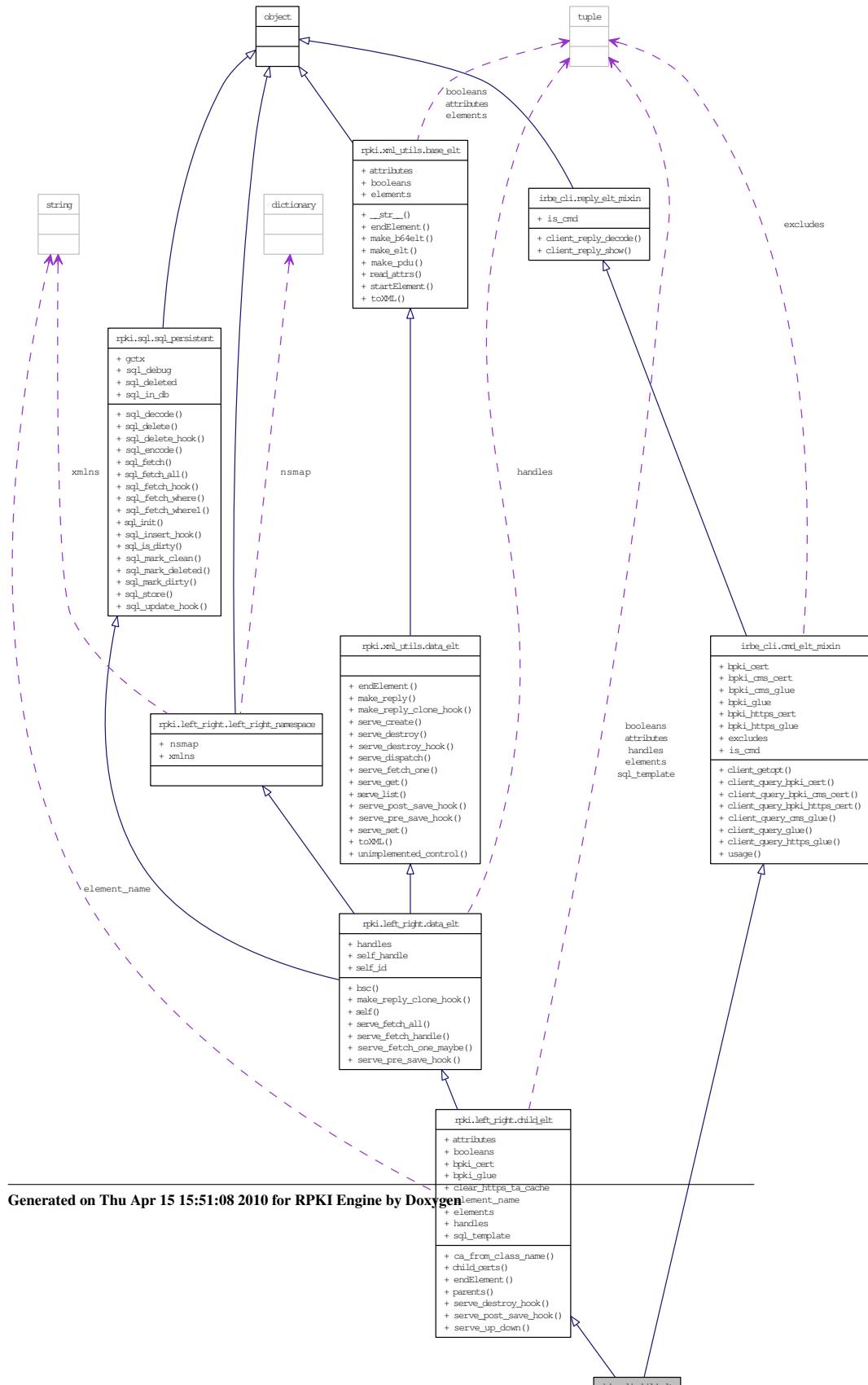
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## 11.7 **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:



### 11.7.1 Detailed Description

Definition at line 174 of file `irbe_cli.py`.

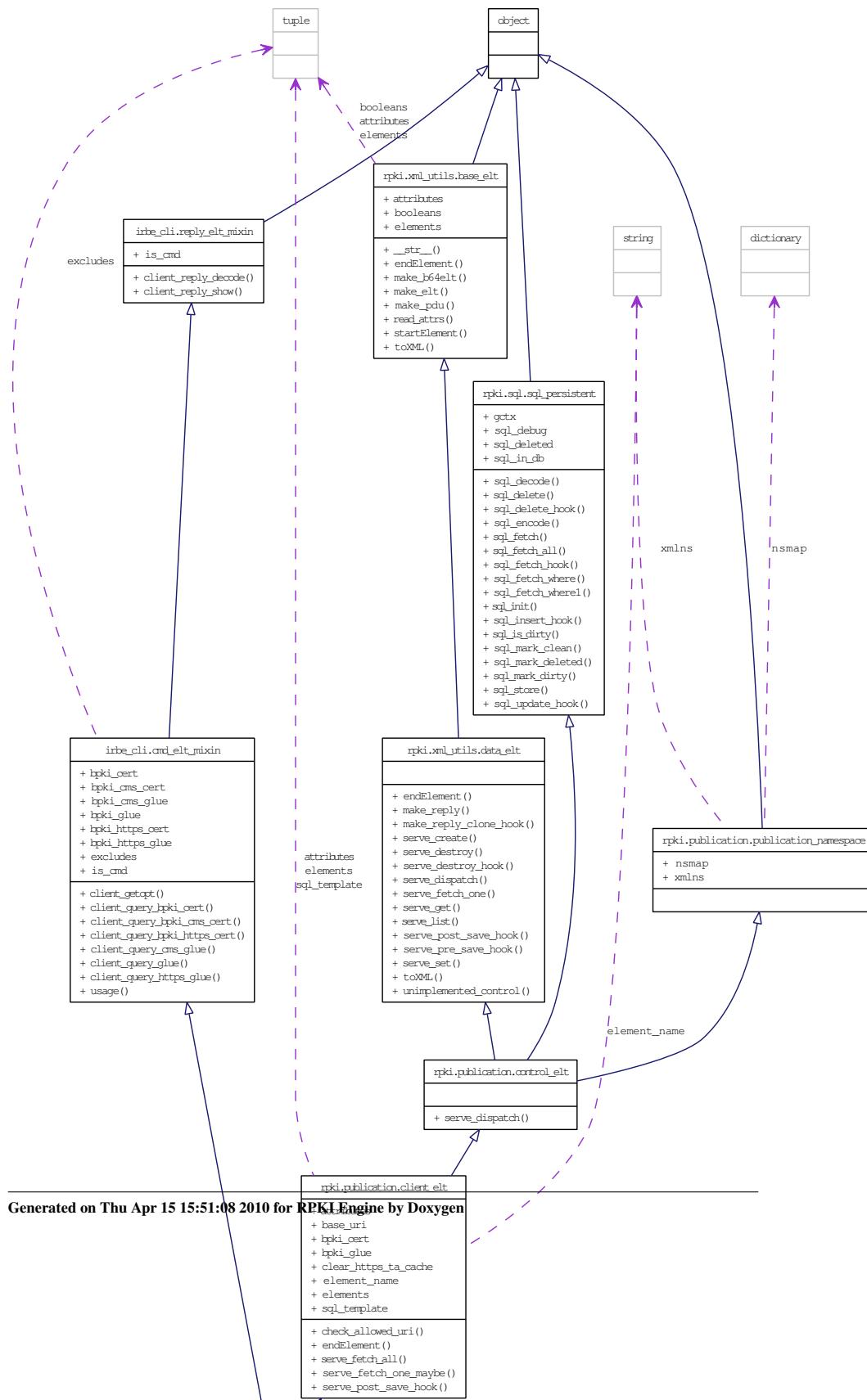
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## 11.8 irbe\_cli.client\_elt Class Reference

Inherits [irbe\\_cli::cmd\\_elt\\_mixin](#), and [rpki::publication::client\\_elt](#).

## Collaboration diagram for irbe\_cli.client\_elt:



### 11.8.1 Detailed Description

Definition at line 208 of file irbe\_cli.py.

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

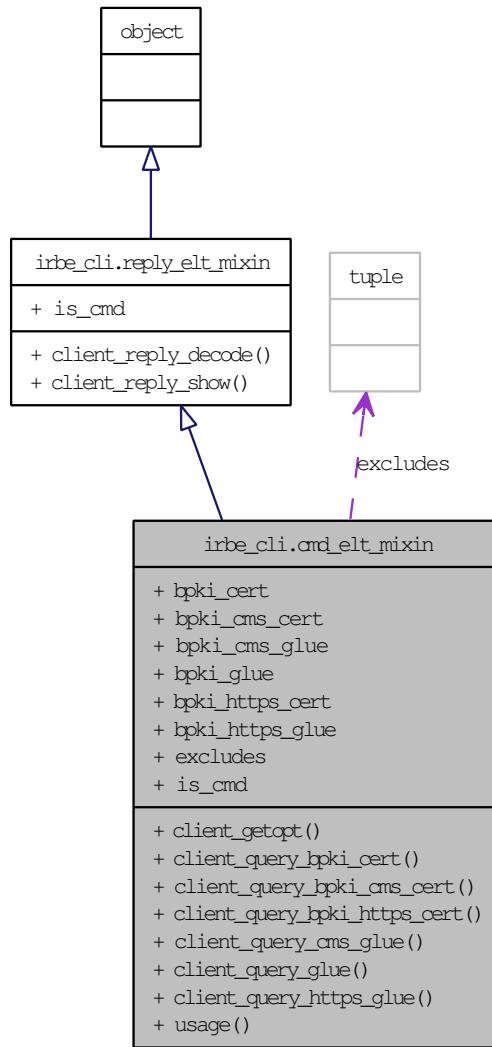
- [irbe\\_cli.py \(3107\)](#)

## 11.9 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

#### 11.9.1 Detailed Description

Protocol mix-in for command line client element PDUs.

Definition at line 68 of file irbe\_cli.py.

#### 11.9.2 Member Function Documentation

##### 11.9.2.1 def `irbe_cli.cmd_elt_mixin.client_getopt (self, argv)`

Parse options for this class.

Definition at line 92 of file irbe\_cli.py.

##### 11.9.2.2 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.

**11.9.2.3 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.

**11.9.2.4 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.

**11.9.2.5 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.

**11.9.2.6 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.

**11.9.2.7 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.

**11.9.2.8 def irbe\_cli.cmd\_elt\_mixin.usage (cls)**

Generate usage message for this PDU.

Definition at line 81 of file irbe\_cli.py.

### 11.9.3 Member Data Documentation

#### 11.9.3.1 `irbe_cli.cmd_elt_mixin.bpk_i_cert`

Definition at line 111 of file `irbe_cli.py`.

#### 11.9.3.2 `irbe_cli.cmd_elt_mixin.bpk_i_cms_cert`

Definition at line 119 of file `irbe_cli.py`.

#### 11.9.3.3 `irbe_cli.cmd_elt_mixin.bpk_i_cms_glue`

Definition at line 123 of file `irbe_cli.py`.

#### 11.9.3.4 `irbe_cli.cmd_elt_mixin.bpk_i_glue`

Definition at line 115 of file `irbe_cli.py`.

#### 11.9.3.5 `irbe_cli.cmd_elt_mixin.bpk_i_https_cert`

Definition at line 127 of file `irbe_cli.py`.

#### 11.9.3.6 `irbe_cli.cmd_elt_mixin.bpk_i_https_glue`

Definition at line 131 of file `irbe_cli.py`.

#### 11.9.3.7 `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.

#### 11.9.3.8 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:

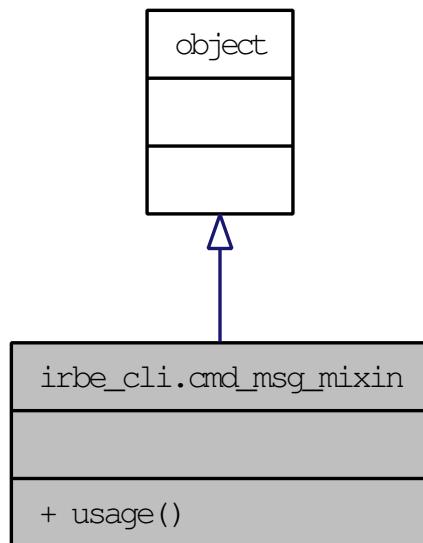
- [irbe\\_cli.py \(3107\)](#)

## 11.10 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](#)

### 11.10.1 Detailed Description

Protocol mix-in for command line client message PDUs.

Definition at line 133 of file irbe\_cli.py.

### 11.10.2 Member Function Documentation

#### 11.10.2.1 def irbe\_cli.cmd\_msg\_mixin.usage ( *cls* )

Generate usage message for this PDU.

Definition at line 139 of file irbe\_cli.py.

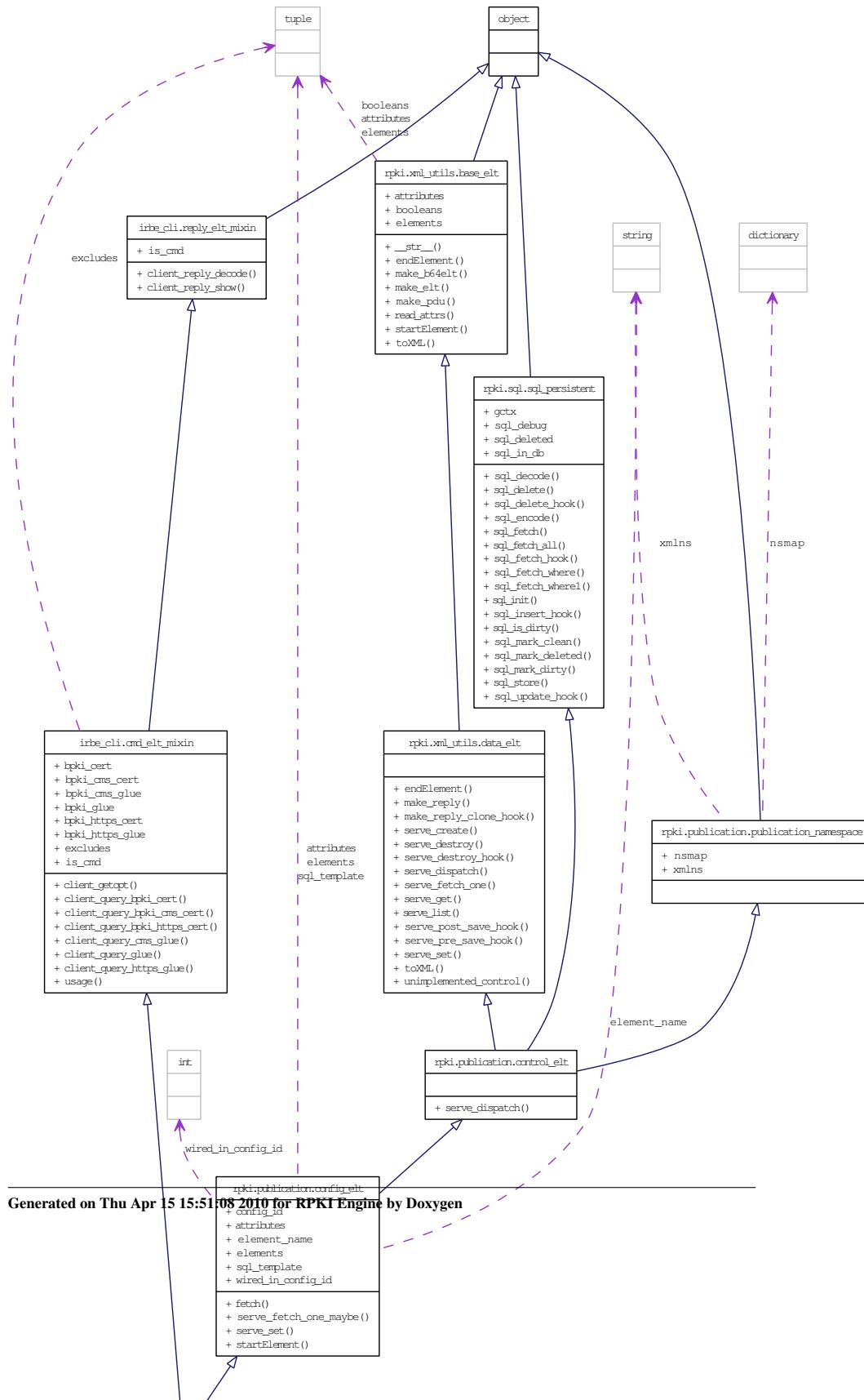
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## 11.11 irbe\_cli.config\_elt Class Reference

Inherits [irbe\\_cli::cmd\\_elt\\_mixin](#), and [rpkib::publication::config\\_elt](#).

Collaboration diagram for irbe\_cli.config\_elt:



**Public Member Functions**

- def [client\\_query\\_bpki\\_crl](#)

**Public Attributes**

- [bpki\\_crl](#)

**11.11.1 Detailed Description**

Definition at line 202 of file irbe\_cli.py.

**11.11.2 Member Function Documentation****11.11.2.1 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.

**11.11.3 Member Data Documentation****11.11.3.1 irbe\_cli.config\_elt.bpkicrl**

Definition at line 206 of file irbe\_cli.py.

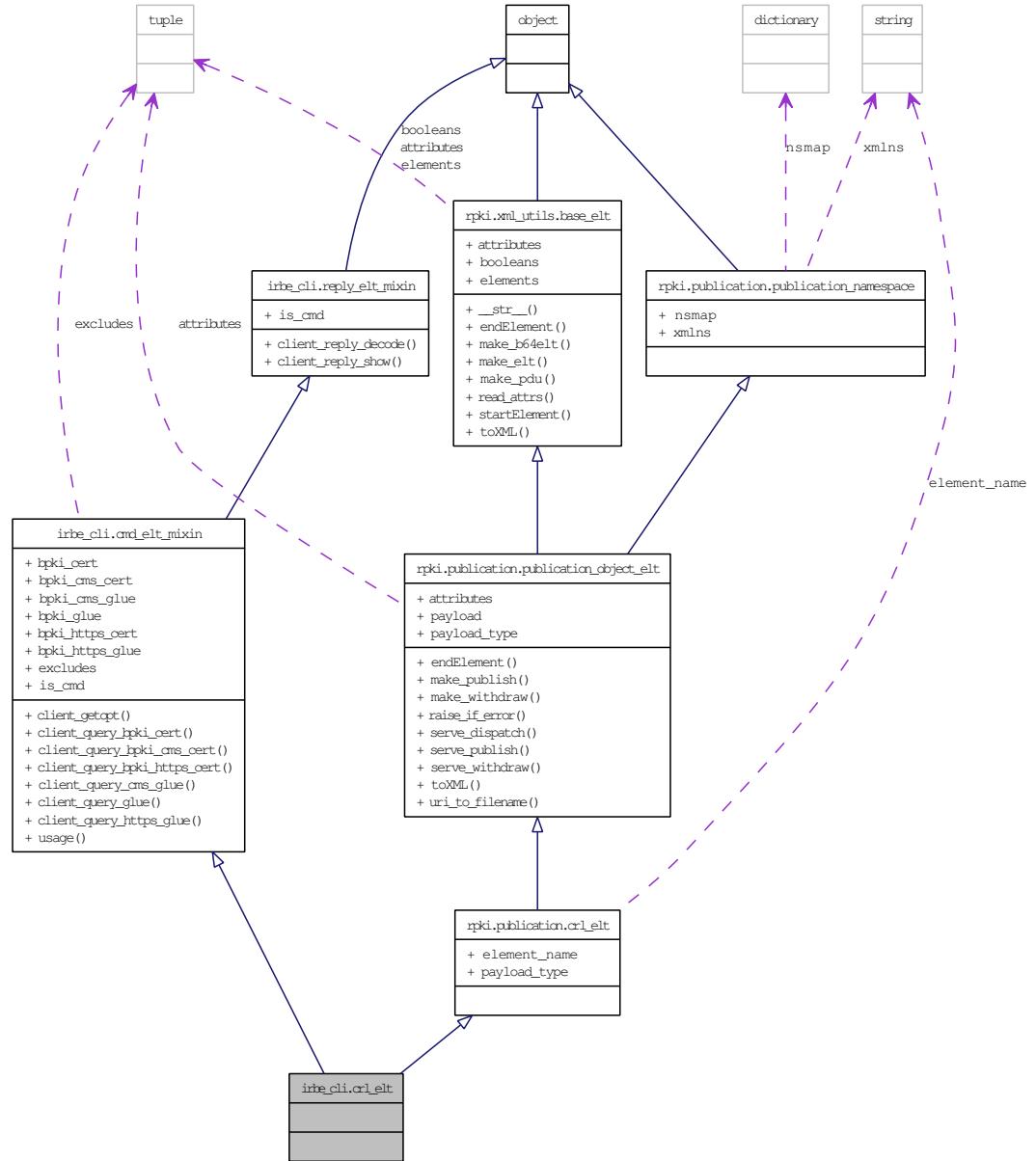
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

**11.12 irbe\_cli.crl\_elt Class Reference**

Inherits [irbe\\_cli::cmd\\_elt\\_mixin](#), and [rpki::publication::crl\\_elt](#).

Collaboration diagram for irbe\_cli.crl\_elt:



### 11.12.1 Detailed Description

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

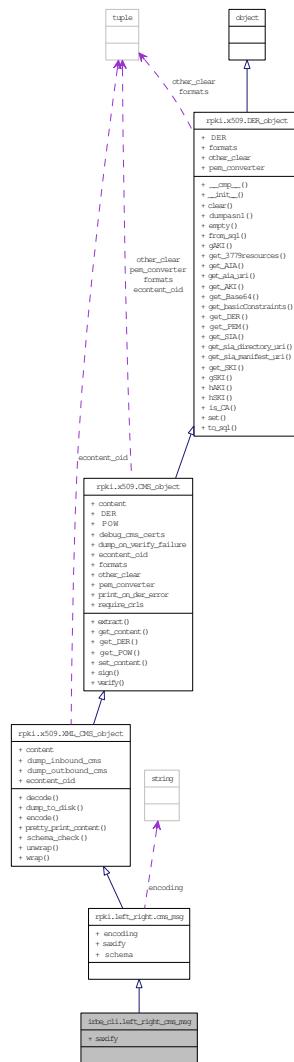
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## 11.13 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`

#### 11.13.1 Detailed Description

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

#### 11.13.2 Member Data Documentation

##### 11.13.2.1 `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`.

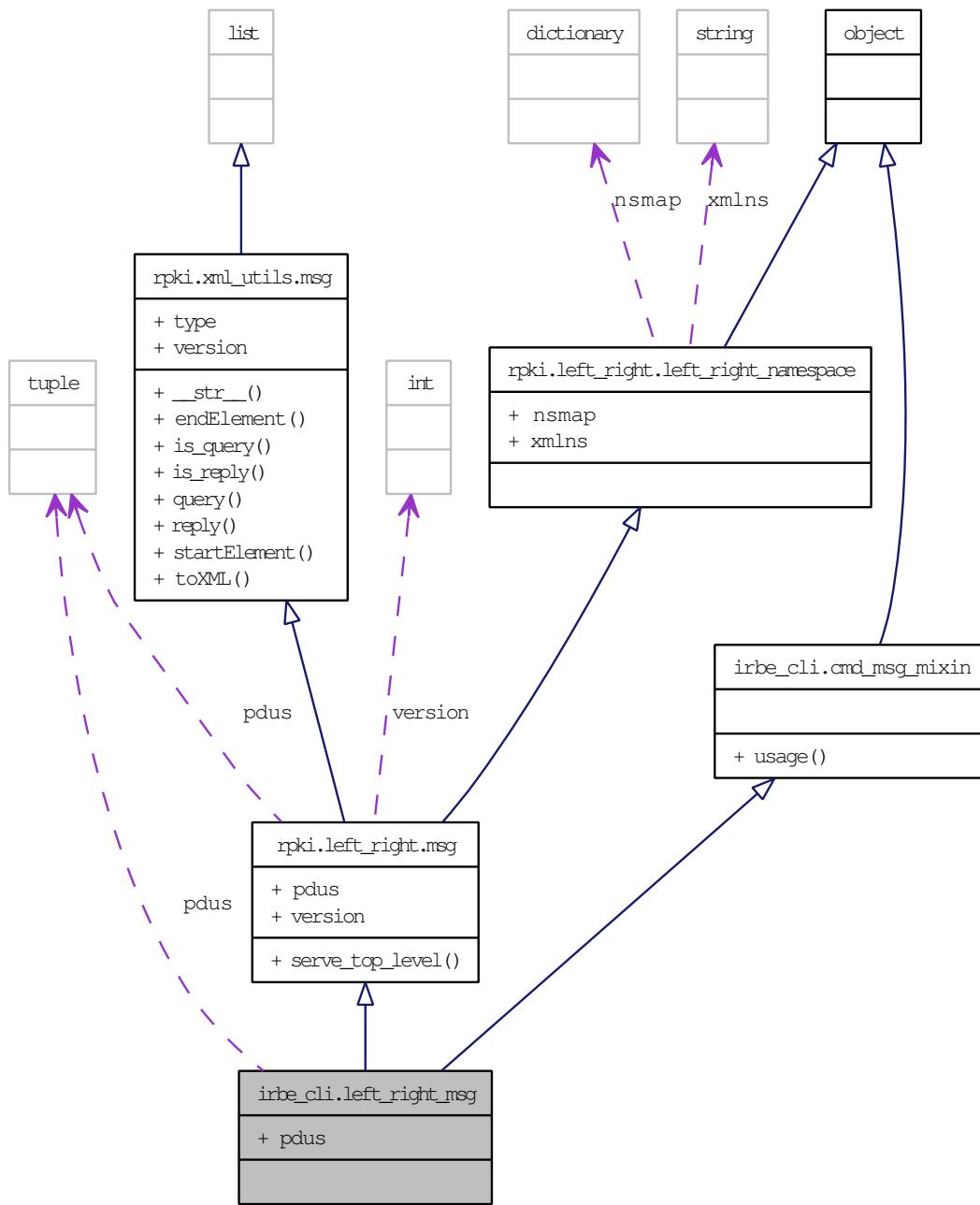
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## 11.14 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.*

#### 11.14.1 Detailed Description

Definition at line 189 of file irbe\_cli.py.

#### 11.14.2 Member Data Documentation

##### 11.14.2.1 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.

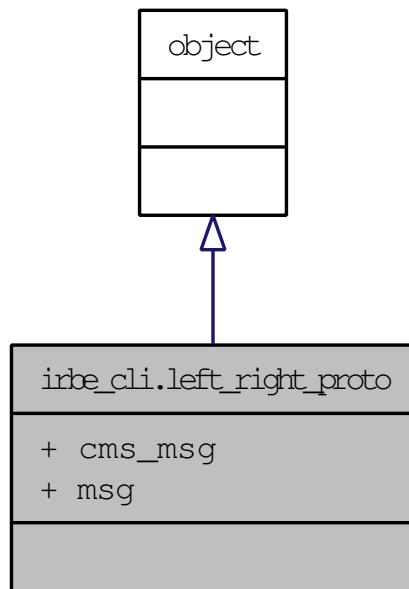
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## 11.15 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`

#### 11.15.1 Detailed Description

Definition at line 302 of file irbe\_cli.py.

#### 11.15.2 Member Data Documentation

##### 11.15.2.1 `irbe_cli.left_right_proto.cms_msg = left_right_cms_msg [static]`

Definition at line 303 of file irbe\_cli.py.

##### 11.15.2.2 `irbe_cli.left_right_proto.msg = left_right_msg [static]`

Definition at line 304 of file irbe\_cli.py.

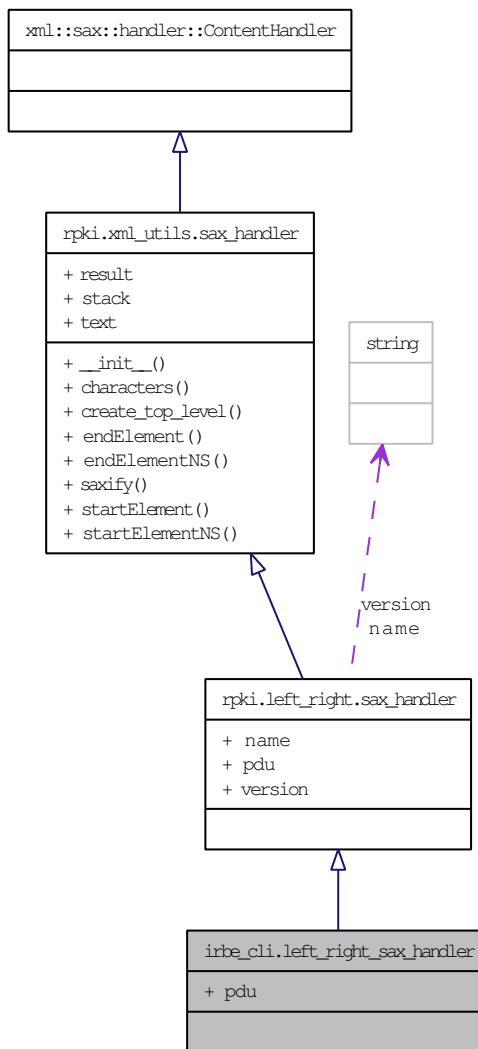
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## 11.16 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](#)

**11.16.1 Detailed Description**

Definition at line 194 of file [irbe\\_cli.py](#).

**11.16.2 Member Data Documentation****11.16.2.1 irbe\_cli.left\_right\_sax\_handler.pdu = left\_right\_msg [static]**

Reimplemented from [rpki.left\\_right.sax\\_handler](#).

Definition at line 195 of file [irbe\\_cli.py](#).

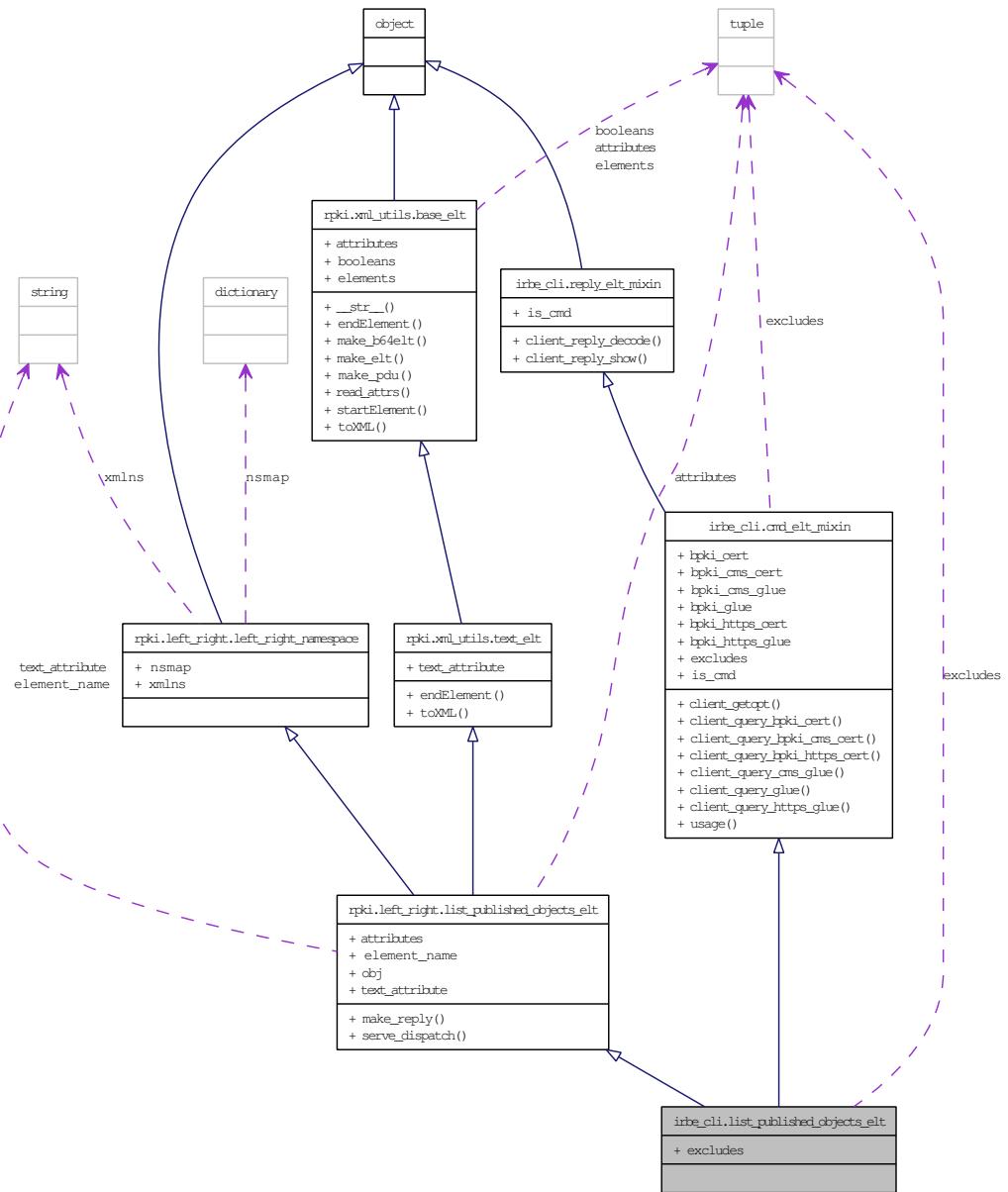
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

**11.17 irbe\_cli.list\_published\_objects\_elt Class Reference**

Inherits [irbe\\_cli::cmd\\_elt\\_mixin](#), and [rpki::left\\_right::list\\_published\\_objects\\_elt](#).

Collaboration diagram for irbe\_cli.list\_published\_objects\_elt:



### Static Public Attributes

- tuple `excludes` = ("uri",)

*XML attributes and elements that should not be allowed as command line arguments.*

### 11.17.1 Detailed Description

Definition at line 180 of file `irbe_cli.py`.

### 11.17.2 Member Data Documentation

#### 11.17.2.1 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`.

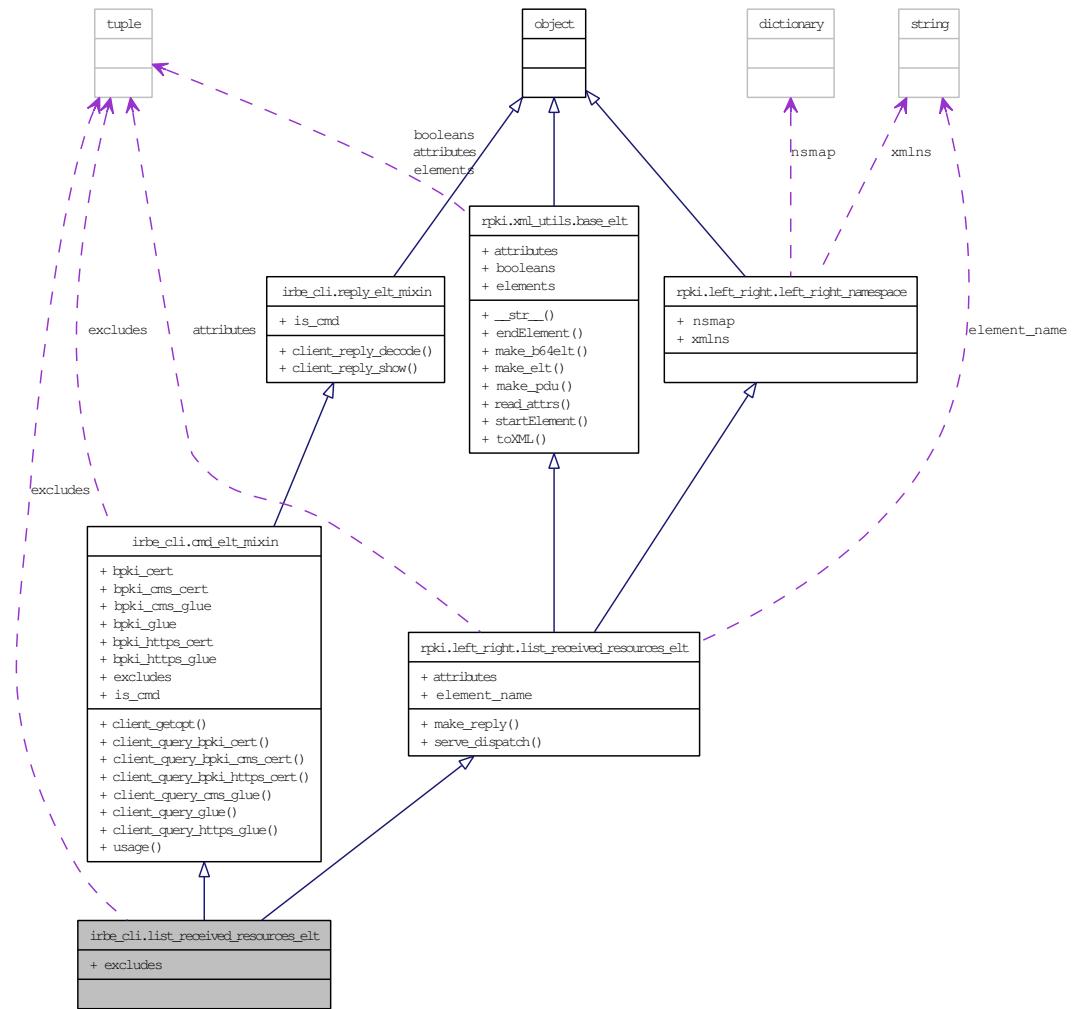
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## 11.18 `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.*

### 11.18.1 Detailed Description

Definition at line 183 of file irbe\_cli.py.

### 11.18.2 Member Data Documentation

**11.18.2.1 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.

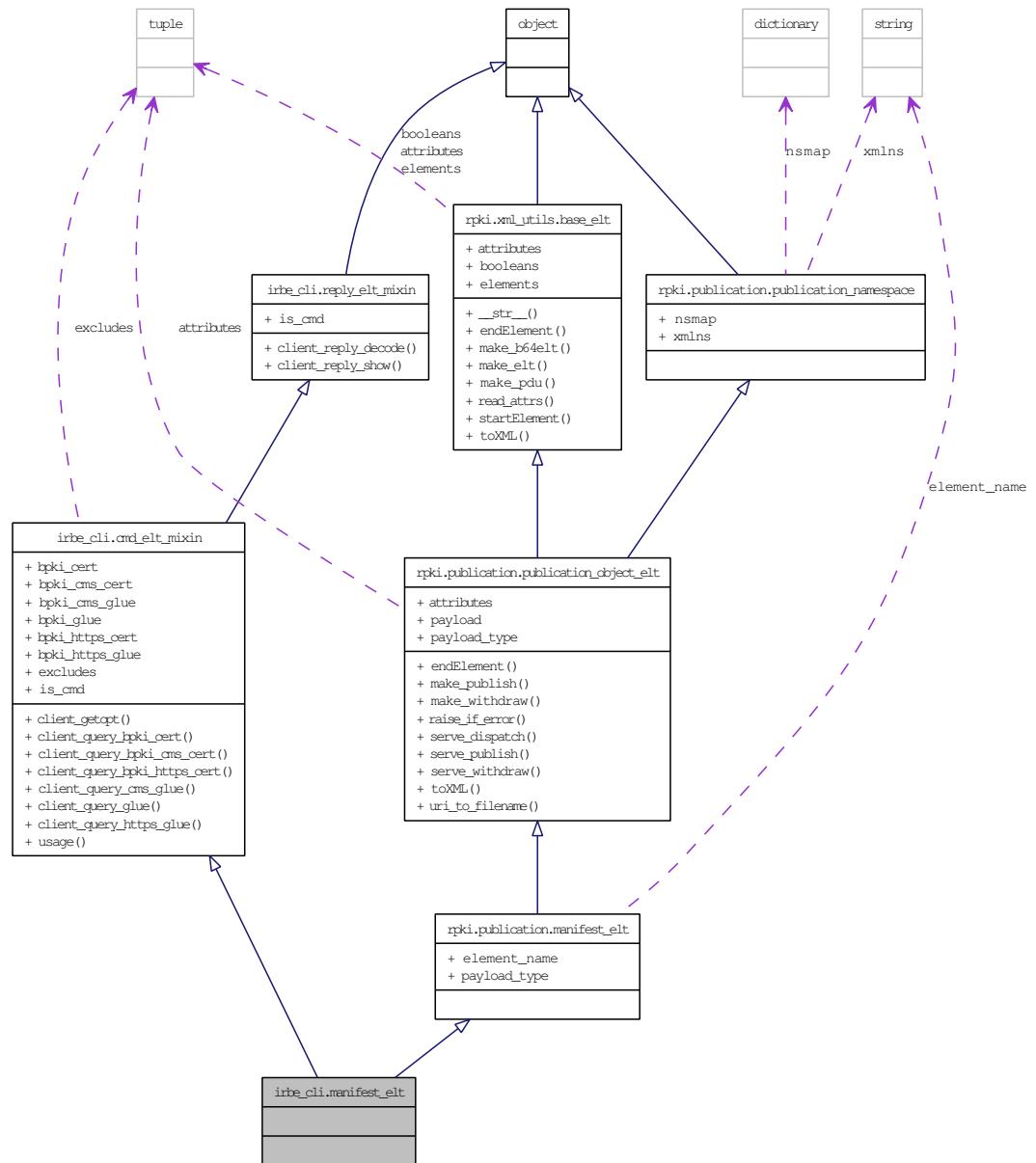
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## 11.19 irbe\_cli.manifest\_elt Class Reference

Inherits [irbe\\_cli::cmd\\_elt\\_mixin](#), and [rpkid::publication::manifest\\_elt](#).

Collaboration diagram for irbe\_cli.manifest\_elt:



### 11.19.1 Detailed Description

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

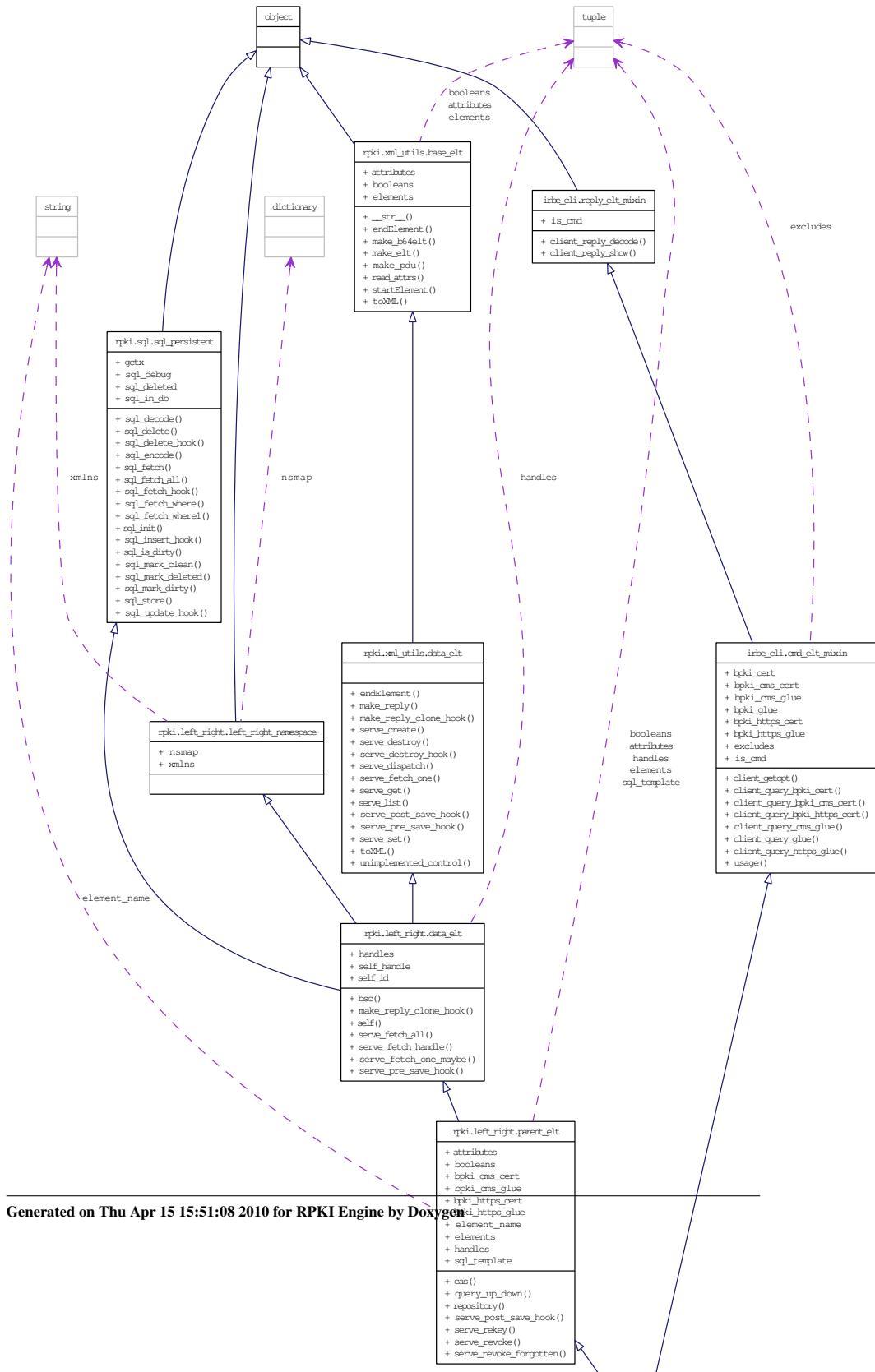
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## 11.20 `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:



### **11.20.1 Detailed Description**

Definition at line 171 of file `irbe_cli.py`.

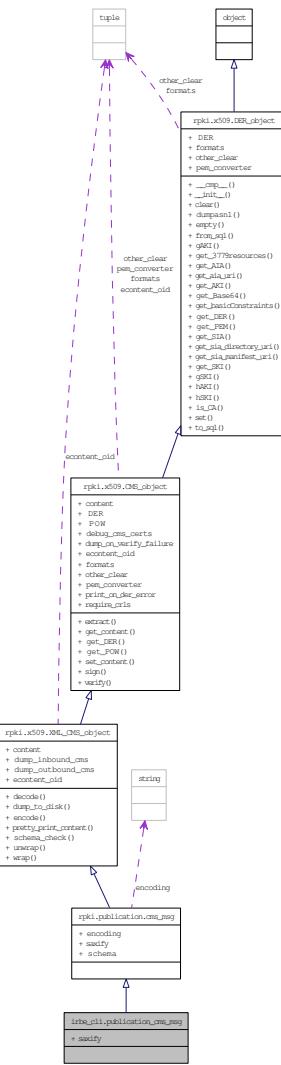
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## **11.21 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`

### **11.21.1 Detailed Description**

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

### 11.21.2 Member Data Documentation

#### 11.21.2.1 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](#).

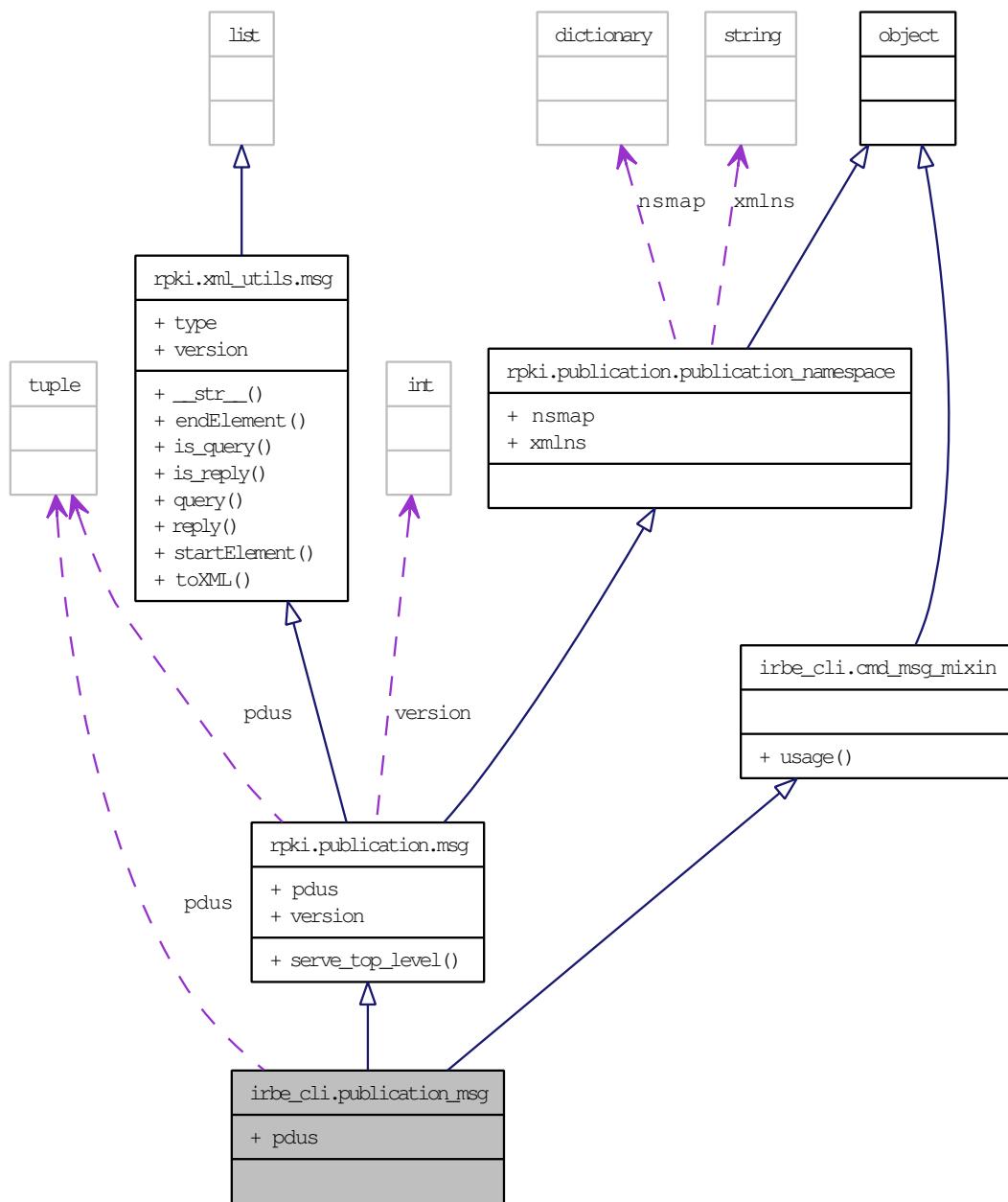
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## 11.22 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.*

#### 11.22.1 Detailed Description

Definition at line 226 of file irbe\_cli.py.

#### 11.22.2 Member Data Documentation

##### 11.22.2.1 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.

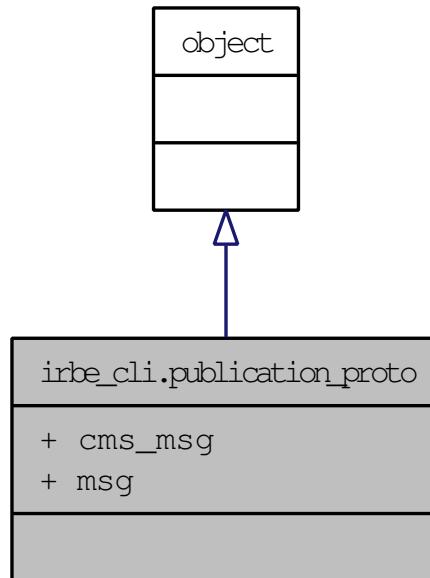
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

### 11.23 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`

#### 11.23.1 Detailed Description

Definition at line 319 of file irbe\_cli.py.

#### 11.23.2 Member Data Documentation

##### 11.23.2.1 `irbe_cli.publication_proto.cms_msg = publication_cms_msg [static]`

Definition at line 321 of file irbe\_cli.py.

##### 11.23.2.2 `irbe_cli.publication_proto.msg = publication_msg [static]`

Definition at line 320 of file irbe\_cli.py.

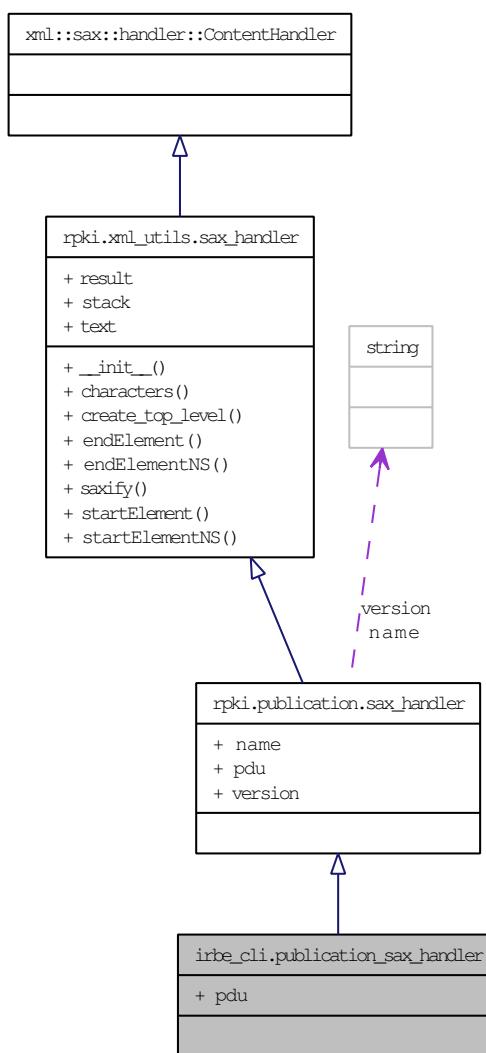
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## 11.24 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](#)

**11.24.1 Detailed Description**

Definition at line 230 of file irbe\_cli.py.

**11.24.2 Member Data Documentation****11.24.2.1 irbe\_cli.publication\_sax\_handler.pdu = publication\_msg [static]**

Reimplemented from [rpki.publication.sax\\_handler](#).

Definition at line 231 of file irbe\_cli.py.

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

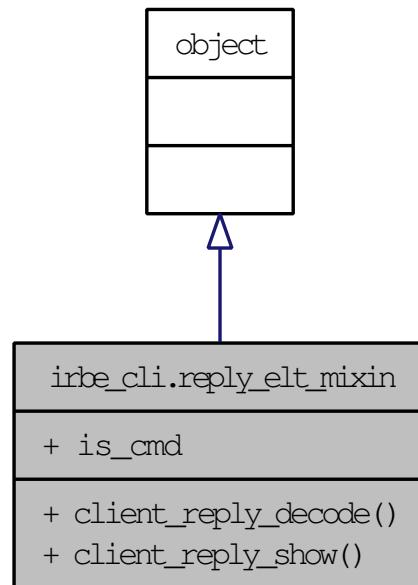
- [irbe\\_cli.py \(3107\)](#)

**11.25 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

### 11.25.1 Detailed Description

Protocol mix-in for printout of reply PDUs.

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

### 11.25.2 Member Function Documentation

#### 11.25.2.1 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](#).

### 11.25.2.2 def irbe\_cli.reply\_elt\_mixin.client\_reply\_show ( *self* )

Definition at line 62 of file [irbe\\_cli.py](#).

## 11.25.3 Member Data Documentation

### 11.25.3.1 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](#).

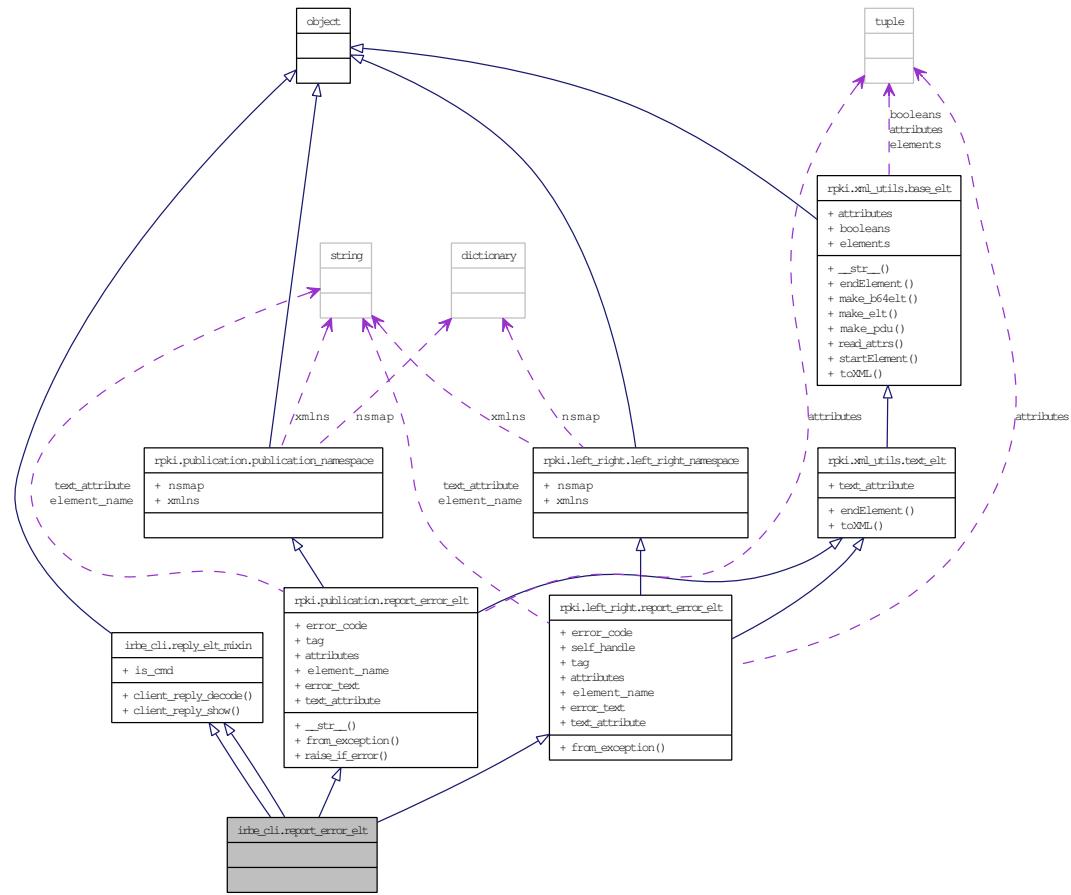
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## 11.26 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:



### 11.26.1 Detailed Description

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

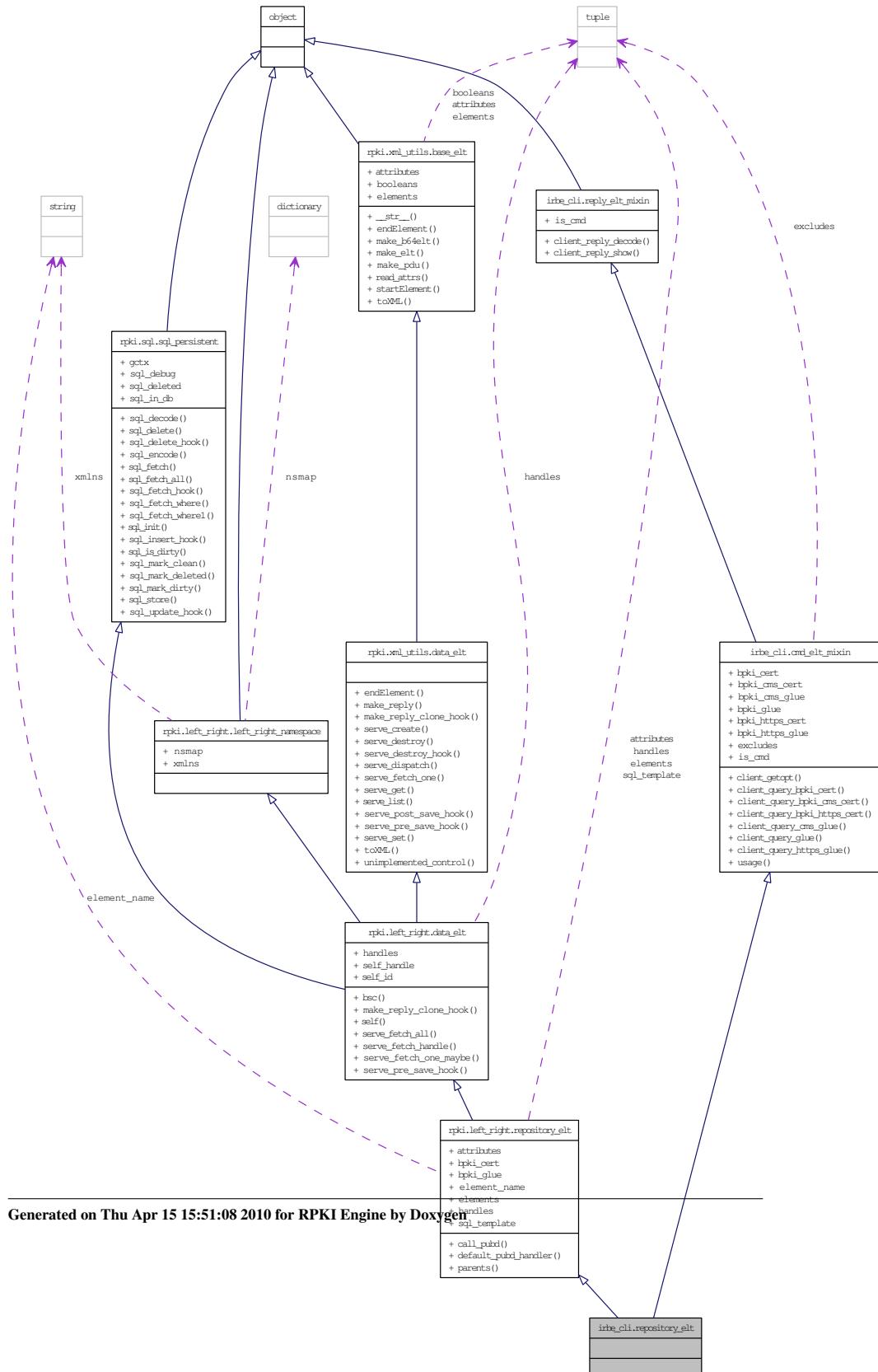
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## 11.27 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:



### **11.27.1 Detailed Description**

Definition at line 177 of file [irbe\\_cli.py](#).

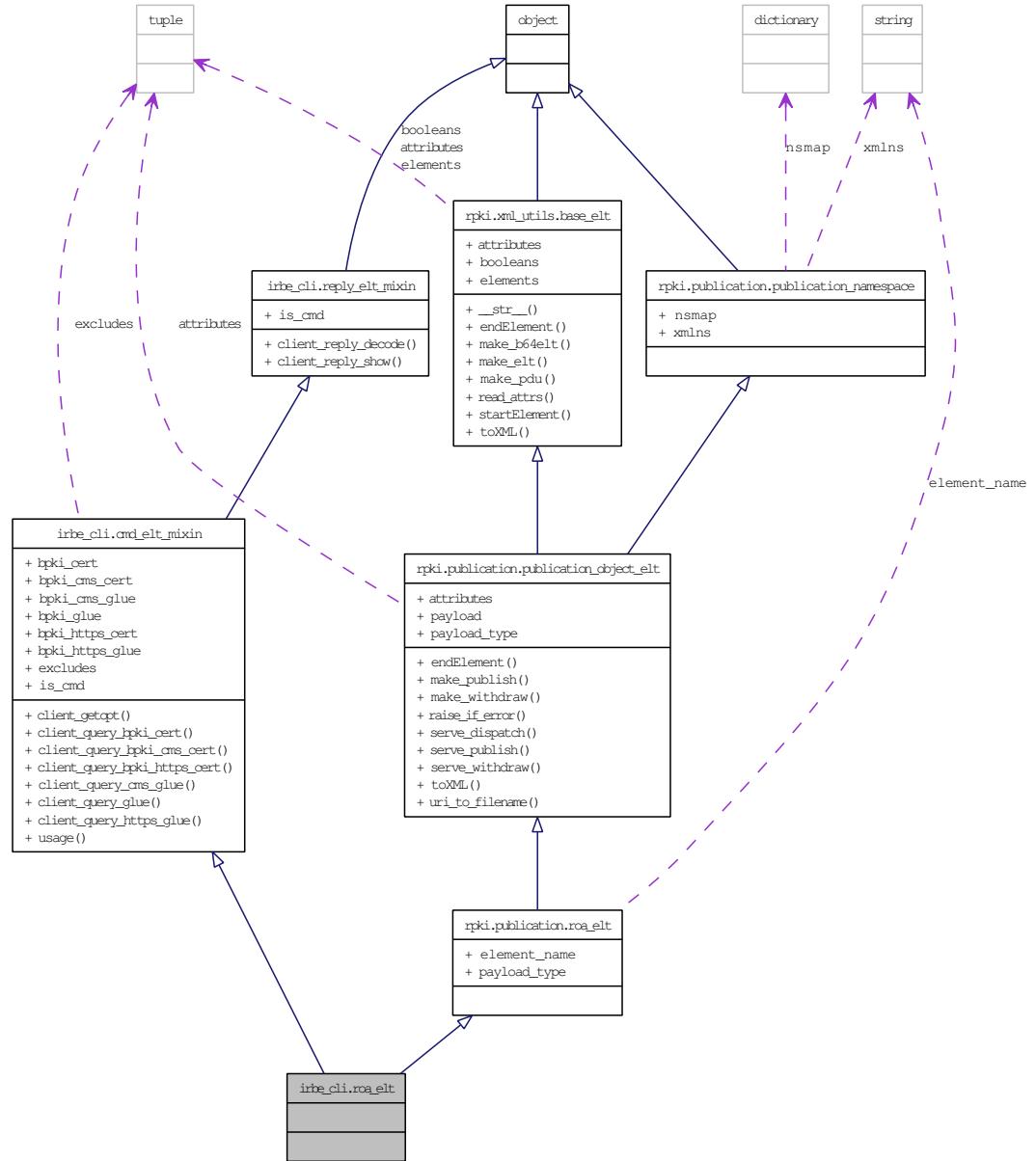
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## **11.28 irbe\_cli.roa\_elt Class Reference**

Inherits [irbe\\_cli::cmd\\_elt\\_mixin](#), and [rpki::publication::roa\\_elt](#).

Collaboration diagram for irbe\_cli.roa\_elt:



### 11.28.1 Detailed Description

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

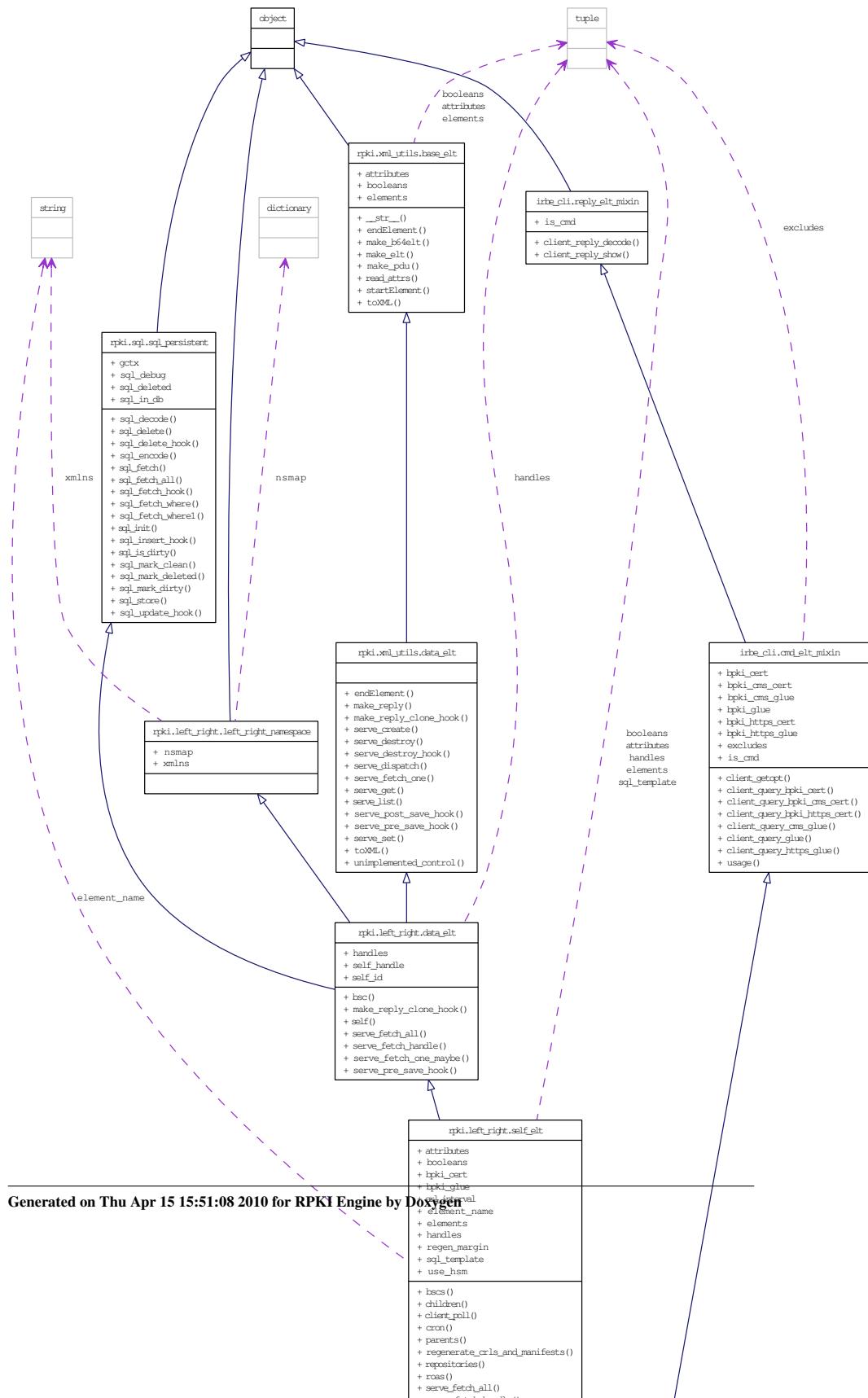
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## **11.29 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:



### 11.29.1 Detailed Description

Definition at line 149 of file irbe\_cli.py.

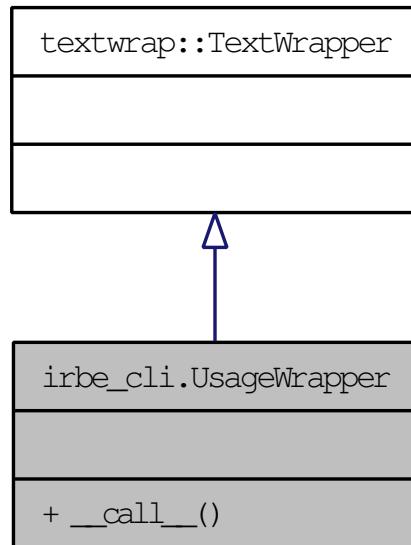
The documentation for this class was generated from the following file:

- [irbe\\_cli.py \(3107\)](#)

## 11.30 irbe\_cli.UsageWrapper Class Reference

Inherits [textwrap::TextWrapper](#).

Collaboration diagram for irbe\_cli.UsageWrapper:



### Public Member Functions

- def [\\_\\_call\\_\\_](#)

### 11.30.1 Detailed Description

Call interface around Python `textwrap.Textwrapper` class.

Definition at line 41 of file irbe\_cli.py.

### 11.30.2 Member Function Documentation

#### 11.30.2.1 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 \(3107\)](#)

## 11.31 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 \(2424\)](#)

## 11.32 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.rpki\\_engine.publication\\_queue](#), [rpki.rpki\\_engine.rpkid\\_context](#), [rpki.sql.session](#), [rpki.sql.sql\\_persistent](#), [rpki.sql.template](#), [rpki.up\\_down.base\\_elt](#), [rpki.x509.DeadDrop](#), [rpki.x509.DER\\_object](#), [rpki.x509.PEM\\_converter](#), and [rpki.xml\\_utils.base\\_elt](#).

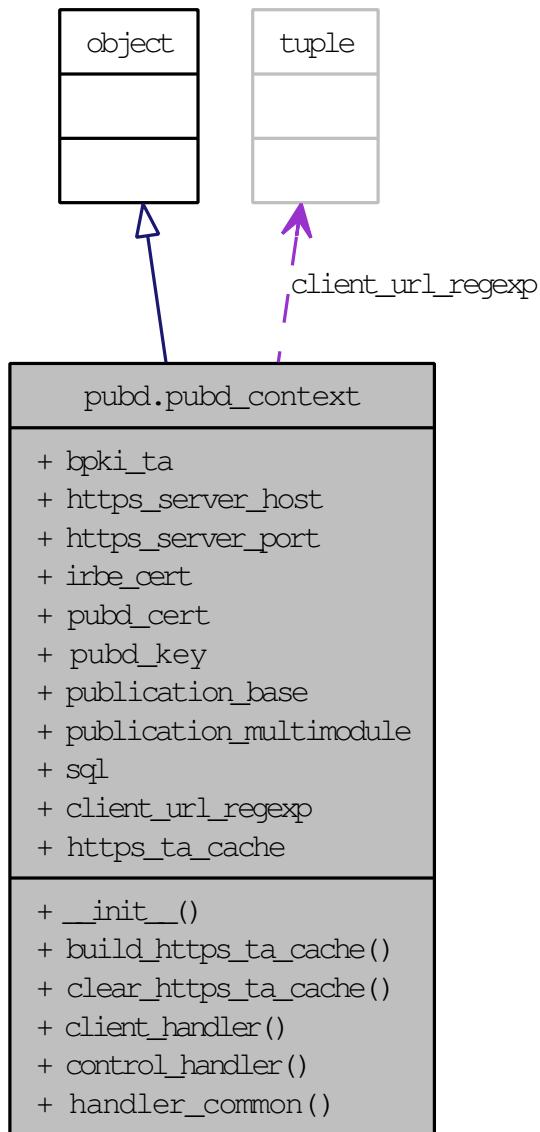
The documentation for this class was generated from the following file:

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

## 11.33 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.*

#### 11.33.1 Detailed Description

A container for various pubd parameters.

Definition at line 46 of file pubd.py.

#### 11.33.2 Member Function Documentation

##### 11.33.2.1 def pubd.pubd\_context.\_\_init\_\_ (self, cfg)

Definition at line 51 of file pubd.py.

##### 11.33.2.2 def pubd.pubd\_context.build\_https\_ta\_cache (self)

Build dynamic TLS trust anchors.

Definition at line 140 of file pubd.py.

**11.33.2.3 def pubd.pubd\_context.clear\_https\_ta\_cache (*self*)**

Clear dynamic TLS trust anchors.

Definition at line 132 of file pubd.py.

**11.33.2.4 def pubd.pubd\_context.client\_handler (*self, query, path, cb*)**

Process one PDU from a client.

Definition at line 100 of file pubd.py.

**11.33.2.5 def pubd.pubd\_context.control\_handler (*self, query, path, cb*)**

Process one PDU from the IRBE.

Definition at line 80 of file pubd.py.

**11.33.2.6 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.

**11.33.3 Member Data Documentation****11.33.3.1 pubd.pubd\_context.bpk\_i\_ta**

Definition at line 55 of file pubd.py.

**11.33.3.2 tuple pubd.pubd\_context.client\_url\_regex =  
re.compile("/client/([-A-Z0-9\_/.]+)\$", re.I) [static]**

Definition at line 98 of file pubd.py.

**11.33.3.3 pubd.pubd\_context.https\_server\_host**

Definition at line 60 of file pubd.py.

**11.33.3.4 pubd.pubd\_context.https\_server\_port**

Definition at line 61 of file pubd.py.

**11.33.3.5 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.

**11.33.3.6 pubd.pubd\_context.irbe\_cert**

Definition at line 56 of file pubd.py.

**11.33.3.7 pubd.pubd\_context.pubd\_cert**

Definition at line 57 of file pubd.py.

**11.33.3.8 pubd.pubd\_context.pubd\_key**

Definition at line 58 of file pubd.py.

**11.33.3.9 pubd.pubd\_context.publication\_base**

Definition at line 63 of file pubd.py.

**11.33.3.10 pubd.pubd\_context.publication\_multimodule**

Definition at line 65 of file pubd.py.

**11.33.3.11 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 \(3107\)](#)

**11.34 datetime Class Reference**

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

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

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

**11.35 timedelta Class Reference**

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

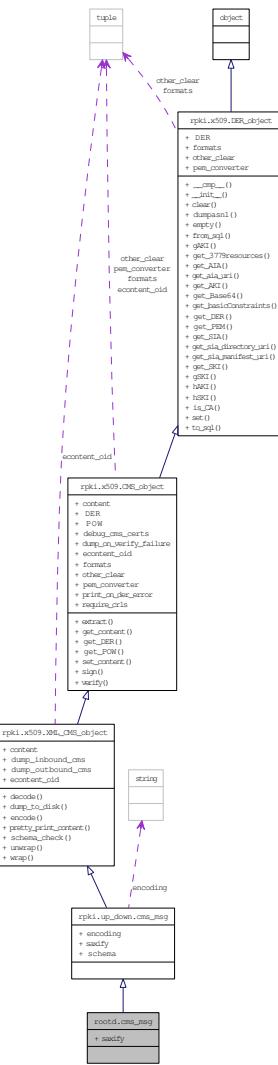
The documentation for this class was generated from the following file:

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

**11.36 rootd.cms\_msg Class Reference**

Inherits [rpki::up\\_down::cms\\_msg](#).

Collaboration diagram for rootd.cms\_msg:



## Static Public Attributes

- `saxify` = `sax_handler.saxify`

### 11.36.1 Detailed Description

Definition at line 235 of file `rootd.py`.

### 11.36.2 Member Data Documentation

#### 11.36.2.1 rootd.cms\_msg.saxify = sax\_handler.saxify [static]

Reimplemented from [rpki.up\\_down.cms\\_msg](#).

Definition at line 236 of file rootd.py.

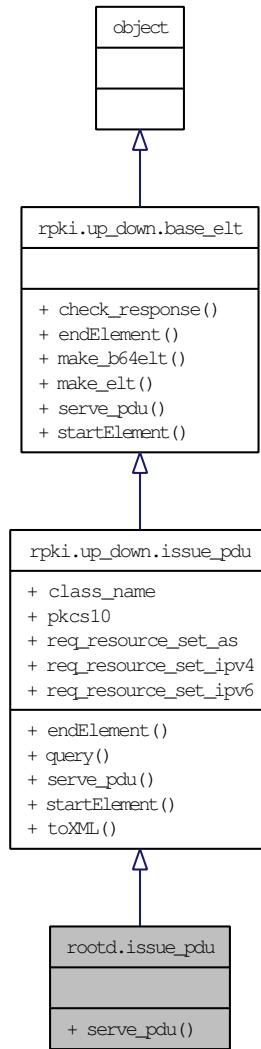
The documentation for this class was generated from the following file:

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

## 11.37 rootd.issue\_pdu Class Reference

Inherits [rpki::up\\_down::issue\\_pdu](#).

Collaboration diagram for rootd.issue\_pdu:



## Public Member Functions

- def [serve\\_pdu](#)

### 11.37.1 Detailed Description

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

### 11.37.2 Member Function Documentation

#### 11.37.2.1 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.

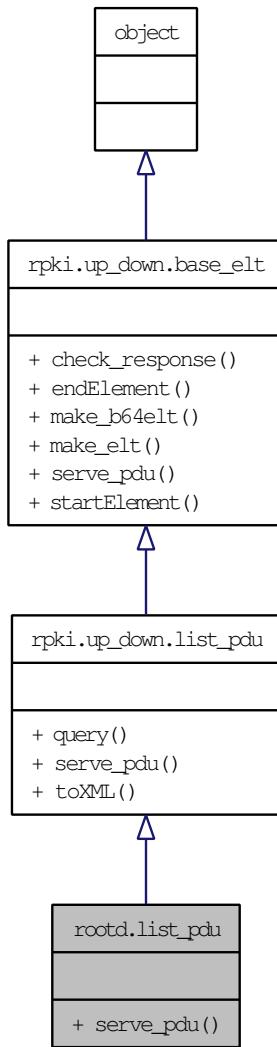
The documentation for this class was generated from the following file:

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

### 11.38 rootd.list\_pdu Class Reference

Inherits [rpki::up\\_down::list\\_pdu](#).

Collaboration diagram for rootd.list\_pdu:



## Public Member Functions

- def [serve\\_pdu](#)

### 11.38.1 Detailed Description

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

### 11.38.2 Member Function Documentation

#### 11.38.2.1 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.

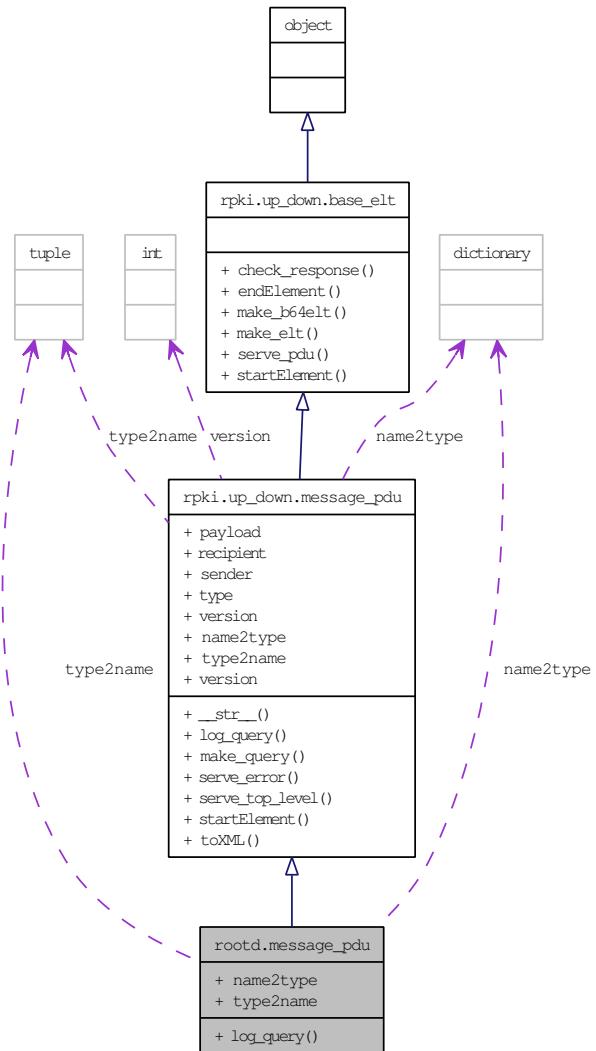
The documentation for this class was generated from the following file:

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

## 11.39 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())

### 11.39.1 Detailed Description

Definition at line 213 of file rootd.py.

### 11.39.2 Member Function Documentation

#### 11.39.2.1 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.

### 11.39.3 Member Data Documentation

#### 11.39.3.1 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.

#### 11.39.3.2 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.

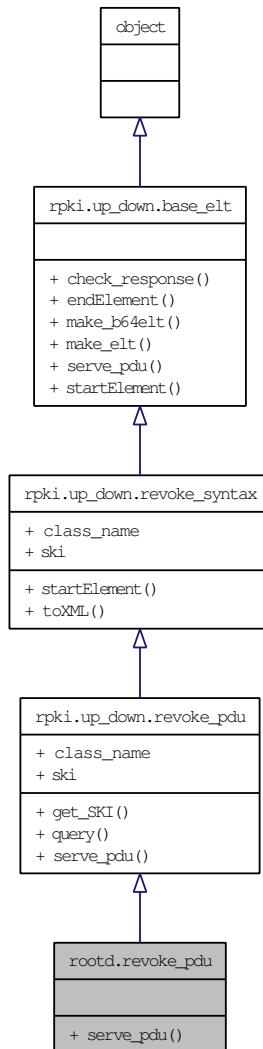
The documentation for this class was generated from the following file:

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

## 11.40 rootd.revocate\_pdu Class Reference

Inherits [rpki::up\\_down::revocate\\_pdu](#).

Collaboration diagram for rootd.revocate\_pdu:



### Public Member Functions

- def [serve\\_pdu](#)

### 11.40.1 Detailed Description

Definition at line 201 of file rootd.py.

### 11.40.2 Member Function Documentation

#### 11.40.2.1 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.

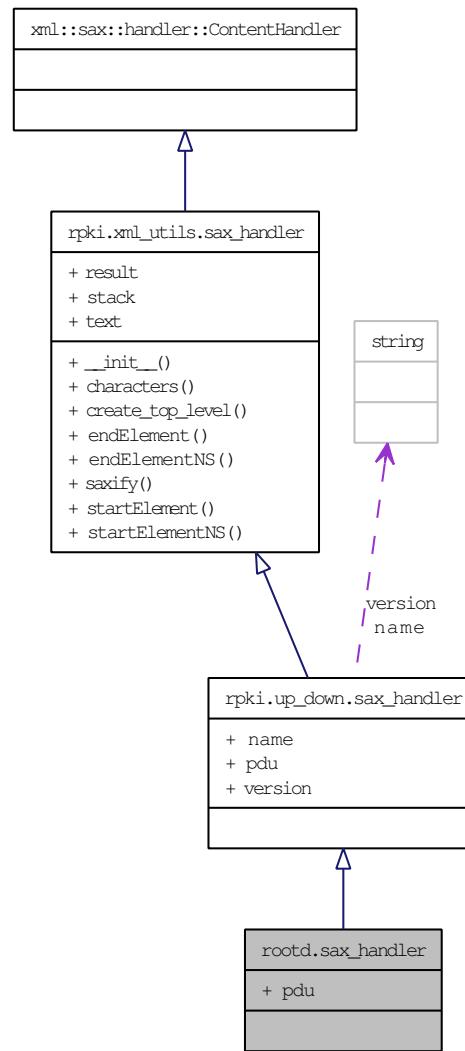
The documentation for this class was generated from the following file:

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

## 11.41 rootd.sax\_handler Class Reference

Inherits [rpki::up\\_down::sax\\_handler](#).

Collaboration diagram for rootd.sax\_handler:



### Static Public Attributes

- `pdu = message_pdu`

#### 11.41.1 Detailed Description

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

### 11.41.2 Member Data Documentation

#### 11.41.2.1 rootd.sax\_handler.pdu = message\_pdu [static]

Reimplemented from [rpkি.up\\_down.sax\\_handler](#).

Definition at line 233 of file rootd.py.

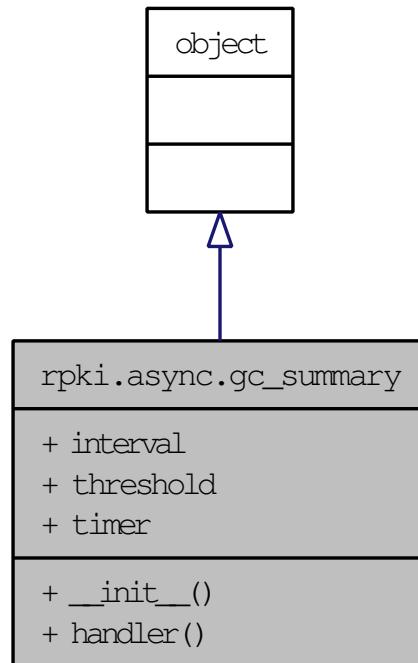
The documentation for this class was generated from the following file:

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

## 11.42 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](#)

#### 11.42.1 Detailed Description

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

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

#### 11.42.2 Member Function Documentation

##### 11.42.2.1 def rpkি.async.gc\_summary.\_\_init\_\_ (*self*, *interval*, *threshold* = 0)

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

##### 11.42.2.2 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`.

#### 11.42.3 Member Data Documentation

##### 11.42.3.1 rpkি.async.gc\_summary.interval

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

##### 11.42.3.2 rpkি.async.gc\_summary.threshold

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

### 11.42.3.3 rpki.async.gc\_summary.timer

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

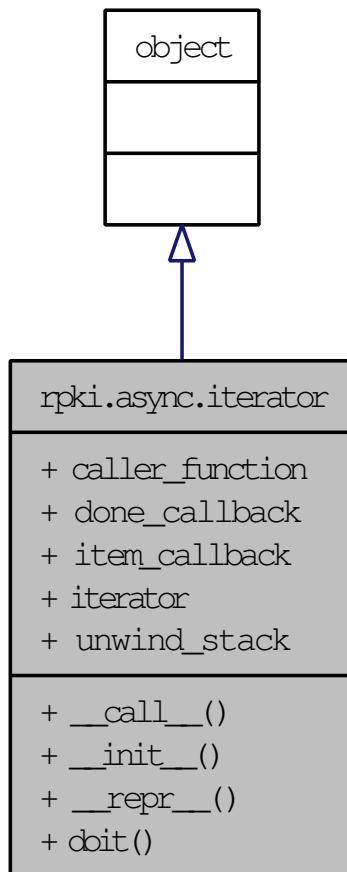
The documentation for this class was generated from the following file:

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

## 11.43 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](#)

### 11.43.1 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`.

### 11.43.2 Member Function Documentation

#### 11.43.2.1 def rpki.async.iterator.\_\_call\_\_ (*self*)

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

**11.43.2.2 def rpki.async.iterator.\_\_init\_\_ ( *self*, *iterable*, *item\_callback*,  
*done\_callback*, *unwind\_stack* = **True**)**

Definition at line 45 of file async.py.

**11.43.2.3 def rpki.async.iterator.\_\_repr\_\_ ( *self*)**

Definition at line 59 of file async.py.

**11.43.2.4 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.

**11.43.3 Member Data Documentation****11.43.3.1 rpki.async.iterator.caller\_function**

Definition at line 48 of file async.py.

**11.43.3.2 rpki.async.iterator.done\_callback**

Definition at line 47 of file async.py.

**11.43.3.3 rpki.async.iterator.item\_callback**

Definition at line 46 of file async.py.

**11.43.3.4 rpki.async.iterator.iterator**

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

**11.43.3.5 rpki.async.iterator.unwind\_stack**

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

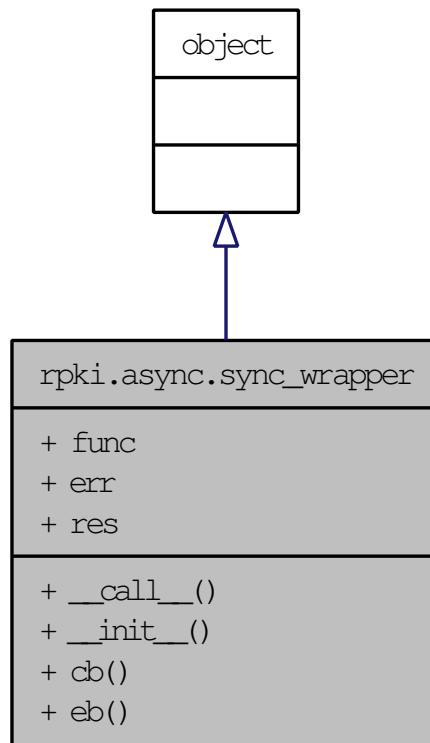
The documentation for this class was generated from the following file:

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

**11.44 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`

### 11.44.1 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`.

### 11.44.2 Member Function Documentation

#### 11.44.2.1 def rpki.async.sync\_wrapper.\_\_call\_\_ (*self*, *args*, *kwargs*)

Definition at line 340 of file `async.py`.

#### 11.44.2.2 def rpki.async.sync\_wrapper.\_\_init\_\_ (*self*, *func*)

Definition at line 320 of file `async.py`.

#### 11.44.2.3 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`.

#### 11.44.2.4 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`.

**11.44.3 Member Data Documentation****11.44.3.1 rpki.async.sync\_wrapper.err = None [static]**

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

**11.44.3.2 rpki.async.sync\_wrapper.func**

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

**11.44.3.3 rpki.async.sync\_wrapper.res = None [static]**

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

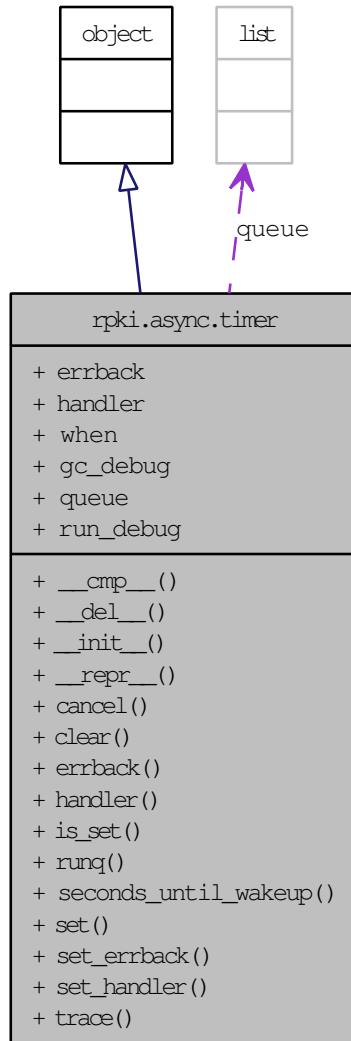
The documentation for this class was generated from the following file:

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

**11.45 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.*

### 11.45.1 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`.

## 11.45.2 Member Function Documentation

### 11.45.2.1 def rpki.async.timer.\_\_cmp\_\_ (*self, other*)

Definition at line 142 of file async.py.

### 11.45.2.2 def rpki.async.timer.\_\_del\_\_ (*self*)

Definition at line 146 of file async.py.

### 11.45.2.3 def rpki.async.timer.\_\_init\_\_ (*self, handler = None, errback = None*)

Definition at line 109 of file async.py.

### 11.45.2.4 def rpki.async.timer.\_\_repr\_\_ (*self*)

Definition at line 209 of file async.py.

### 11.45.2.5 def rpki.async.timer.cancel (*self*)

Cancel a timer, if it was set.

Definition at line 149 of file async.py.

### 11.45.2.6 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.

**11.45.2.7 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`.

**11.45.2.8 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`.

**11.45.2.9 def rpki.async.timer.is\_set (*self*)**

Test whether this timer is currently set.

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

**11.45.2.10 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`.

**11.45.2.11 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`.

**11.45.2.12 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.

**11.45.2.13 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.

**11.45.2.14 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.

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

Debug logging.

Definition at line 118 of file async.py.

**11.45.3 Member Data Documentation****11.45.3.1 rpki.async.timer.errback**

Definition at line 190 of file async.py.

**11.45.3.2 rpkic::async.timer::gc\_debug = False [static]**

Verbose chatter about timers states and garbage collection.

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

**11.45.3.3 rpkic.async.timer.handler**

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

**11.45.3.4 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`.

**11.45.3.5 rpkic::async.timer::run\_debug = False [static]**

Verbose chatter about timers being run.

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

**11.45.3.6 rpkic.async.timer.when**

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

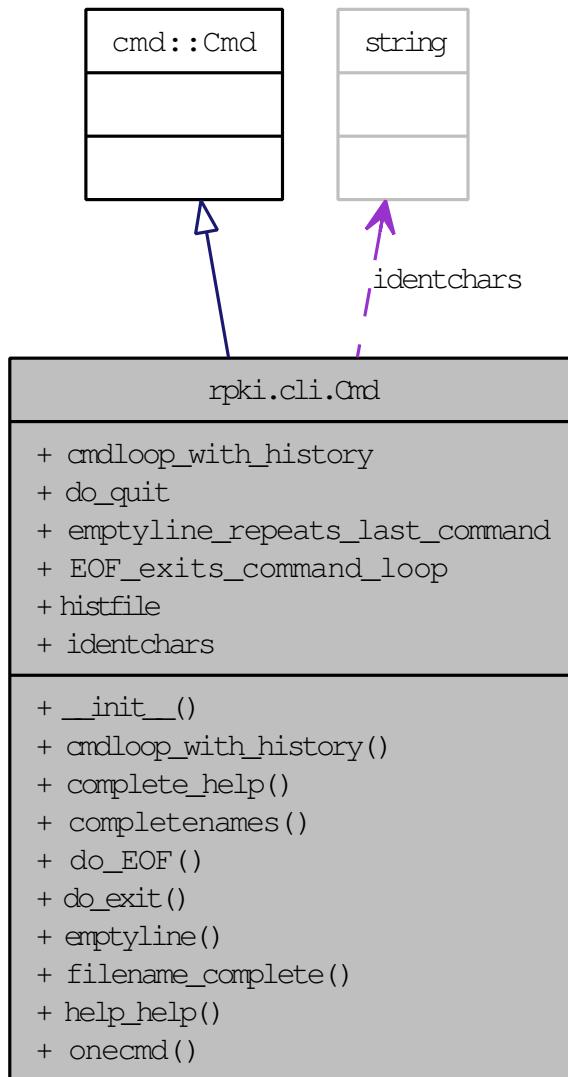
The documentation for this class was generated from the following file:

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

**11.46 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` = "/-."

#### 11.46.1 Detailed Description

Customized subclass of Python cmd module.

Definition at line 29 of file cli.py.

#### 11.46.2 Member Function Documentation

##### 11.46.2.1 def rpki.cli.Cmd.\_\_init\_\_ ( *self*, *argv* = **None**)

Definition at line 42 of file cli.py.

##### 11.46.2.2 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.

**11.46.2.3 def rpki.cli.Cmd.complete\_help (*self*, *args*)**

Better completion function for help command arguments.

Definition at line 119 of file cli.py.

**11.46.2.4 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.

**11.46.2.5 def rpki.cli.Cmd.do\_EOF (*self*, *arg*)**

Exit program.

Definition at line 61 of file cli.py.

**11.46.2.6 def rpki.cli.Cmd.do\_exit (*self*, *arg*)**

Exit program.

Definition at line 69 of file cli.py.

**11.46.2.7 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.

**11.46.2.8 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.

**11.46.2.9 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.

**11.46.2.10 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.

**11.46.3 Member Data Documentation****11.46.3.1 rpki.cli.Cmd.cmdloop\_with\_history = cmd.Cmd.cmdloop  
[static]**

Definition at line 153 of file cli.py.

**11.46.3.2 rpki.cli.Cmd.do\_quit = do\_exit [static]**

Definition at line 75 of file cli.py.

**11.46.3.3 rpki.cli.Cmd.emptyline\_repeats\_last\_command = False [static]**

Definition at line 34 of file cli.py.

**11.46.3.4 rpki.cli.Cmd.EOF\_exits\_command\_loop = True [static]**

Definition at line 36 of file cli.py.

**11.46.3.5 rpki.cli.Cmd.histfile = None [static]**

Definition at line 40 of file cli.py.

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

Definition at line 38 of file cli.py.

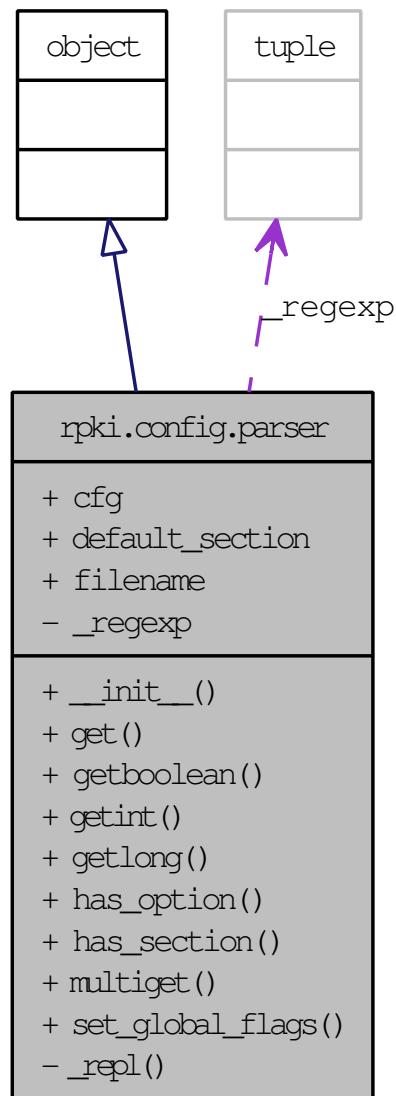
The documentation for this class was generated from the following file:

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

**11.47 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("``\\${(.\*)?::(.\*)?}``")

#### 11.47.1 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.

#### 11.47.2 Member Function Documentation

##### 11.47.2.1 def rpki.config.parser.\_\_init\_\_ ( *self*, *filename*, *section* = **None**, *allow\_missing* = **False**)

Initialize this parser.

Definition at line 50 of file config.py.

**11.47.2.2 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.

**11.47.2.3 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.

**11.47.2.4 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.

**11.47.2.5 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.

**11.47.2.6 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.

**11.47.2.7 def rpki.config.parser.has\_option (*self*, *option*, *section* = **None**)**

Test whether an option exists.

Definition at line 71 of file config.py.

**11.47.2.8 def rpki.config.parser.has\_section (*self*, *section*)**

Test whether a section exists.

Definition at line 64 of file config.py.

**11.47.2.9 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.

**11.47.2.10 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.

**11.47.3 Member Data Documentation****11.47.3.1 tuple rpki.config.parser.\_regexp = re.compile("\\\\${(.\*)::(.\*)}")  
[static, private]**

Definition at line 99 of file config.py.

**11.47.3.2 rpki.config.parser.cfg**

Definition at line 56 of file config.py.

**11.47.3.3 rpki.config.parser.default\_section**

Definition at line 62 of file config.py.

**11.47.3.4 rpki.config.parser.filename**

Definition at line 55 of file config.py.

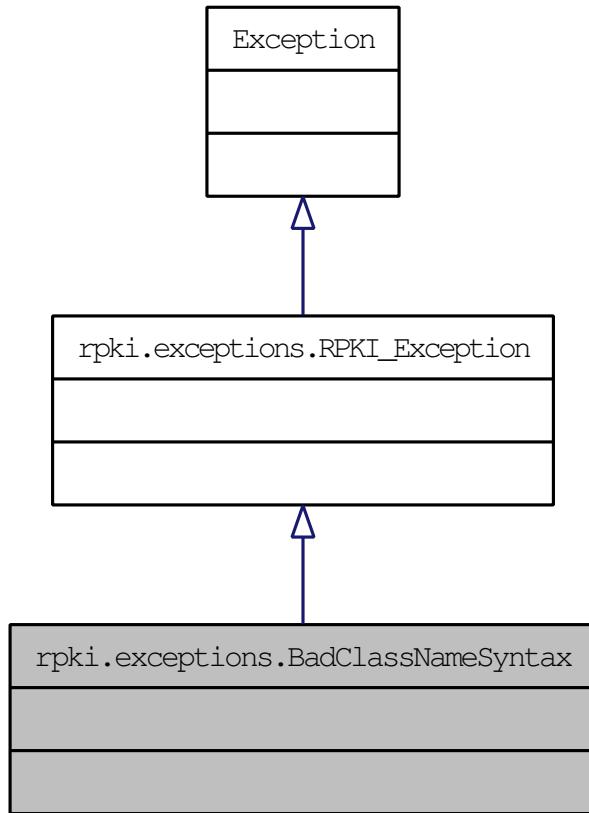
The documentation for this class was generated from the following file:

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

**11.48 rpki.exceptions.BadClassNameSyntax Class Reference**

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.BadClassNameSyntax:



#### 11.48.1 Detailed Description

Illegal syntax for a class\_name.

Definition at line 92 of file exceptions.py.

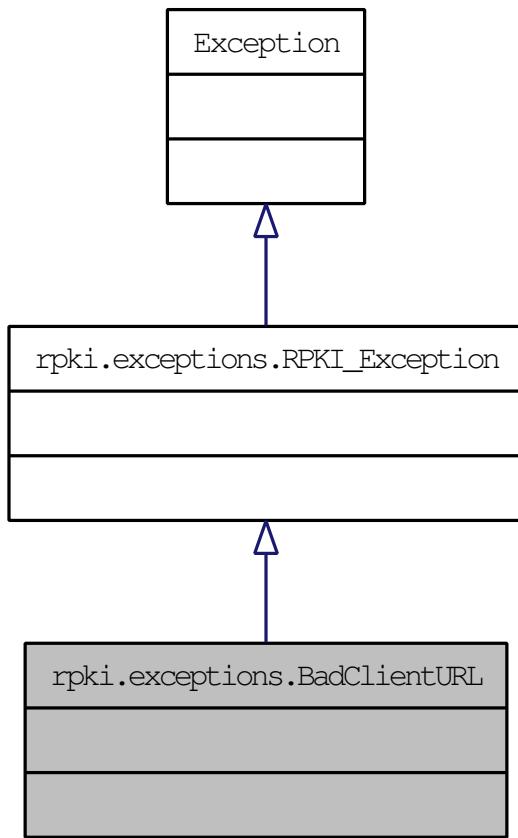
The documentation for this class was generated from the following file:

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

#### 11.49 rpki.exceptions.BadClientURL Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.BadClientURL:



### 11.49.1 Detailed Description

URL given to HTTPS client does not match profile.

Definition at line 232 of file exceptions.py.

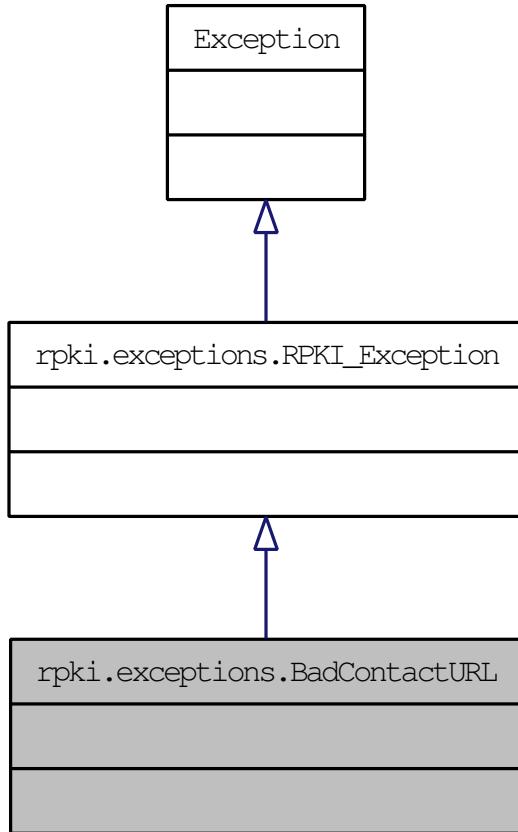
The documentation for this class was generated from the following file:

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

## 11.50 rpki.exceptions.BadContactURL Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.BadContactURL:



### 11.50.1 Detailed Description

Error trying to parse contact URL.

Definition at line 87 of file exceptions.py.

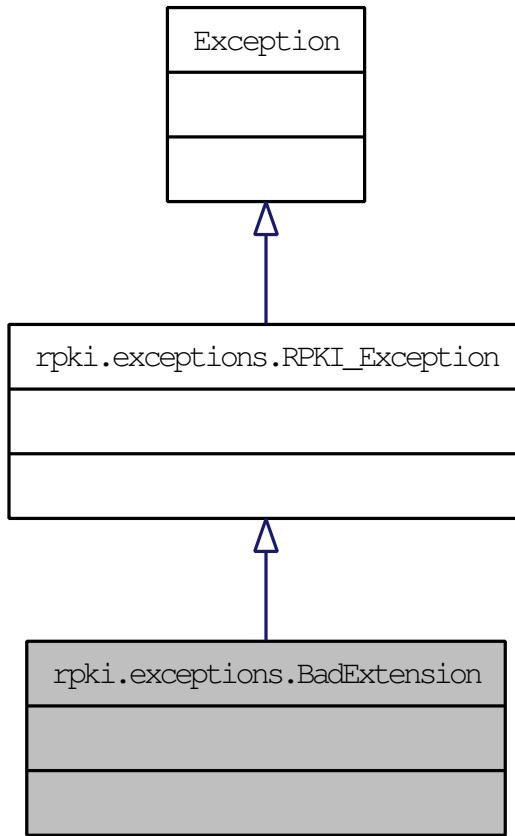
The documentation for this class was generated from the following file:

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

## 11.51 rpki.exceptions.BadExtension Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.BadExtension:



### 11.51.1 Detailed Description

Forbidden X.509 extension.

Definition at line 242 of file exceptions.py.

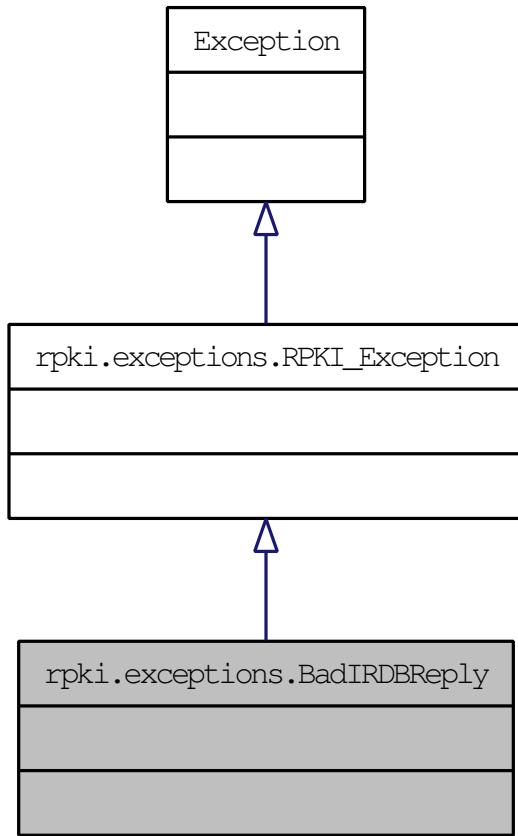
The documentation for this class was generated from the following file:

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

## 11.52 rpki.exceptions.BadIRDBReply Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.BadIRDBReply:



### 11.52.1 Detailed Description

Unexpected reply to IRDB query.

Definition at line 152 of file exceptions.py.

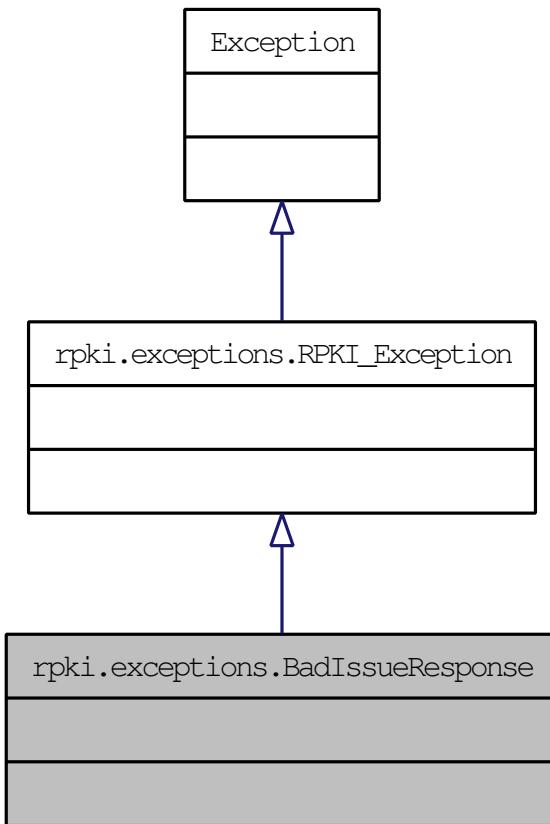
The documentation for this class was generated from the following file:

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

## 11.53 rpki.exceptions.BadIssueResponse Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpkி.exceptions.BadIssueResponse:



### 11.53.1 Detailed Description

`issue_response PDU with wrong number of classes or certificates.`

Definition at line 97 of file `exceptions.py`.

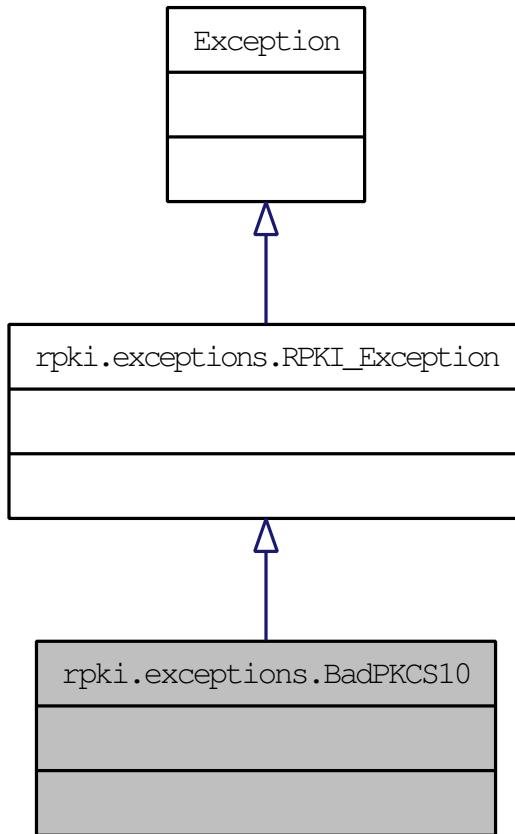
The documentation for this class was generated from the following file:

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

## 11.54 rpkி.exceptions.BadPKCS10 Class Reference

Inherits [rpkி.exceptions.RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.BadPKCS10:



#### 11.54.1 Detailed Description

Bad PKCS #10 object.

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

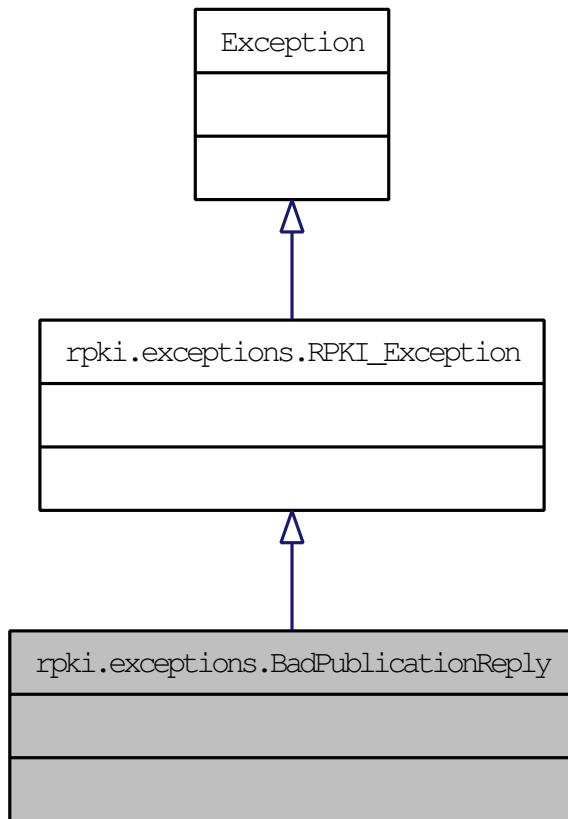
The documentation for this class was generated from the following file:

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

## 11.55 rpki.exceptions.BadPublicationReply Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpkி.exceptions.BadPublicationReply:



### 11.55.1 Detailed Description

Unexpected reply to publication query.

Definition at line 257 of file exceptions.py.

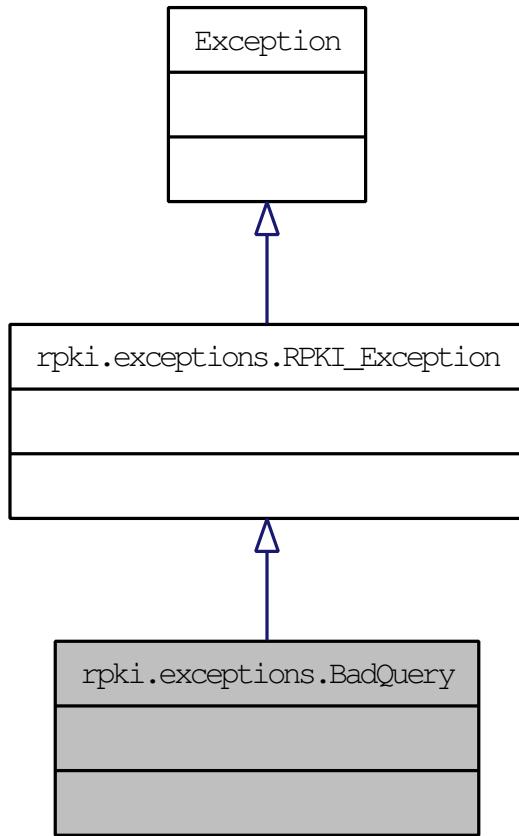
The documentation for this class was generated from the following file:

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

## 11.56 rpkி.exceptions.BadQuery Class Reference

Inherits [rpkி::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.BadQuery:



### 11.56.1 Detailed Description

Unexpected protocol query.

Definition at line 55 of file exceptions.py.

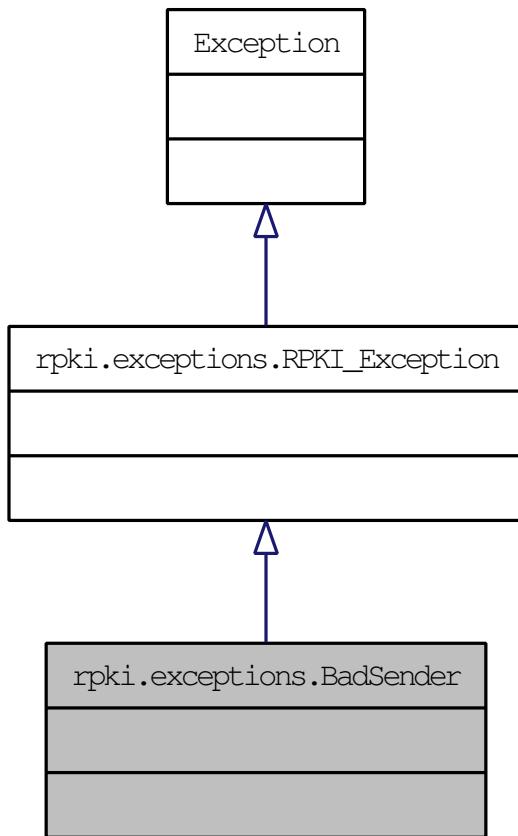
The documentation for this class was generated from the following file:

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

## 11.57 rpki.exceptions.BadSender Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.BadSender:



### 11.57.1 Detailed Description

Unexpected XML sender value.

Definition at line 127 of file exceptions.py.

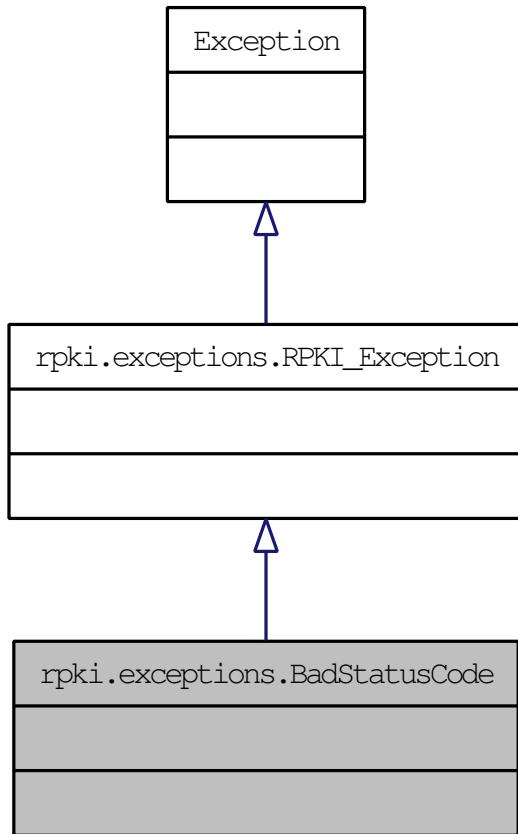
The documentation for this class was generated from the following file:

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

## 11.58 rpki.exceptions.BadStatusCode Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.BadStatusCode:



### 11.58.1 Detailed Description

Unrecognized protocol status code.

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

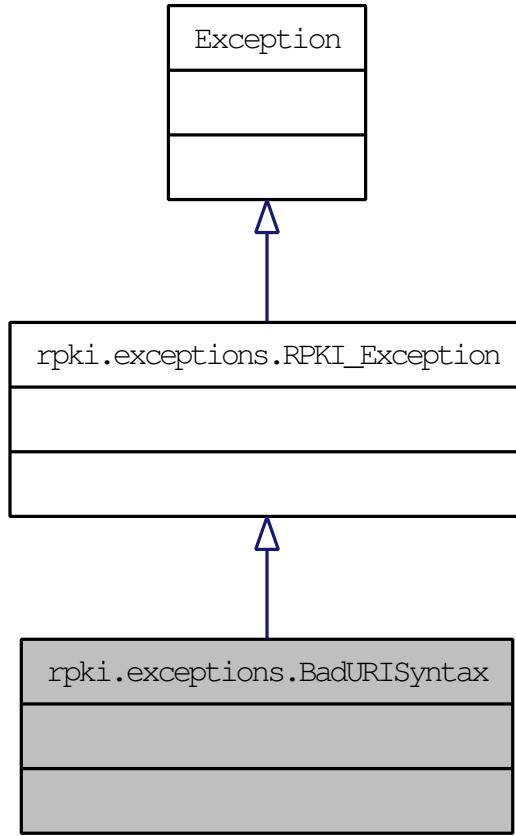
The documentation for this class was generated from the following file:

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

## 11.59 rpki.exceptions.BadURISyntax Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.BadURISyntax:



### 11.59.1 Detailed Description

Illegal syntax for a URI.

Definition at line 45 of file `exceptions.py`.

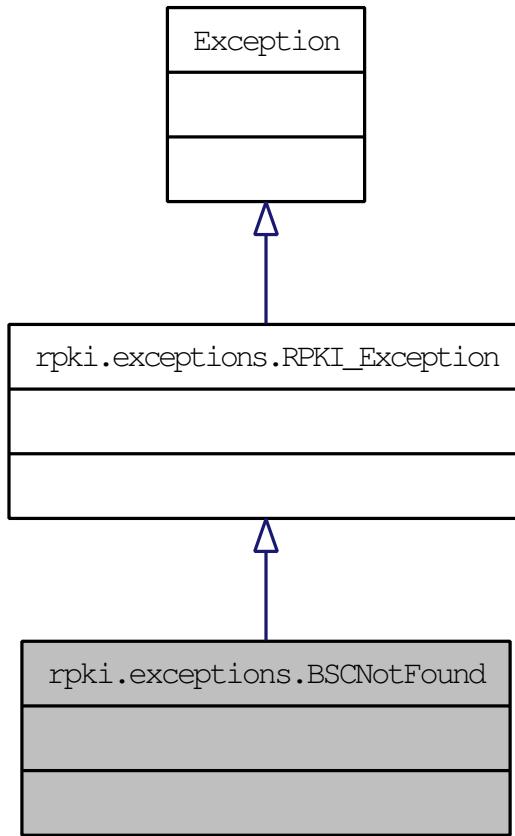
The documentation for this class was generated from the following file:

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

## 11.60 rpki.exceptions.BSCNotFound Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.BSCNotFound:



### 11.60.1 Detailed Description

Could not find specified BSC in database.

Definition at line 122 of file exceptions.py.

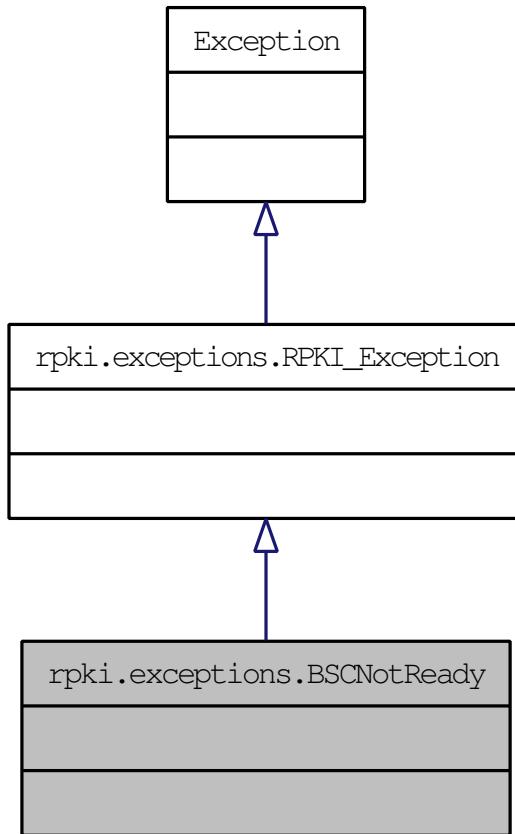
The documentation for this class was generated from the following file:

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

## 11.61 rpki.exceptions.BSCNotReady Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.BSCNotReady:



### 11.61.1 Detailed Description

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

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

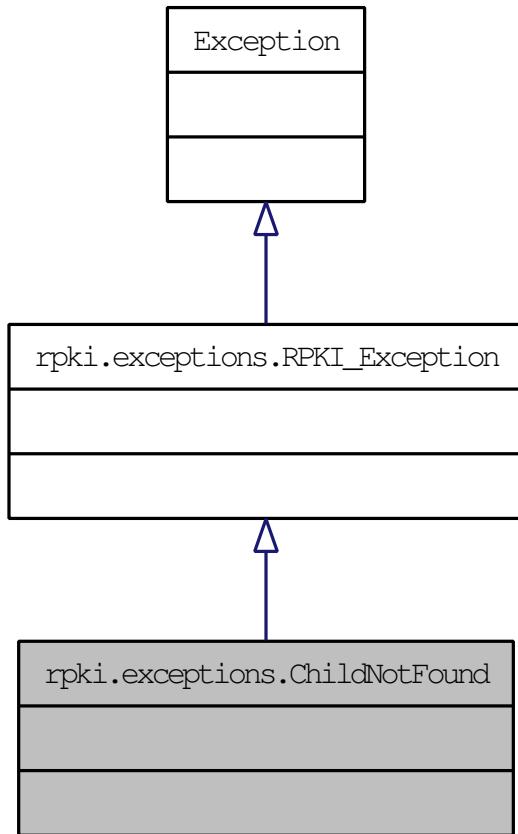
The documentation for this class was generated from the following file:

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

## 11.62 rpki.exceptions.ChildNotFound Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.ChildNotFound:



### 11.62.1 Detailed Description

Could not find specified child in database.

Definition at line 117 of file exceptions.py.

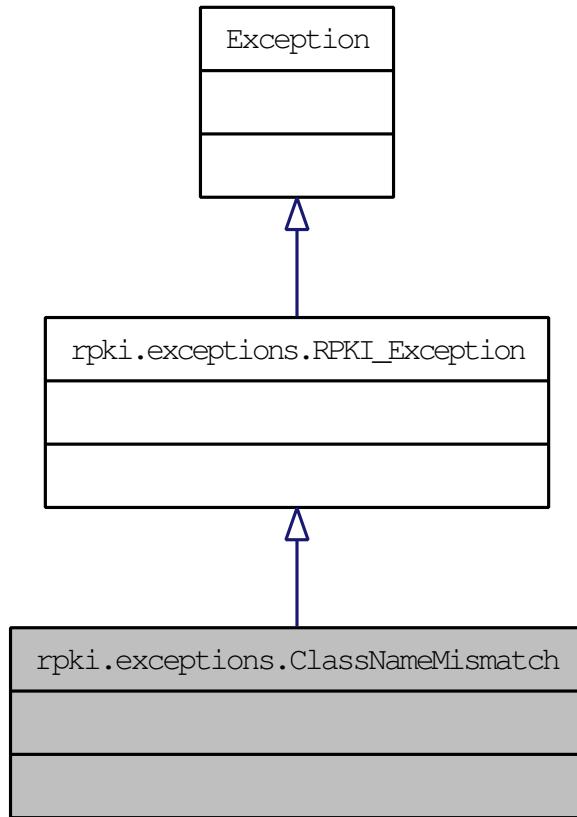
The documentation for this class was generated from the following file:

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

## 11.63 rpki.exceptions.ClassNameMismatch Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.ClassNameMismatch:



### 11.63.1 Detailed Description

`class_name` does not match child context.

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

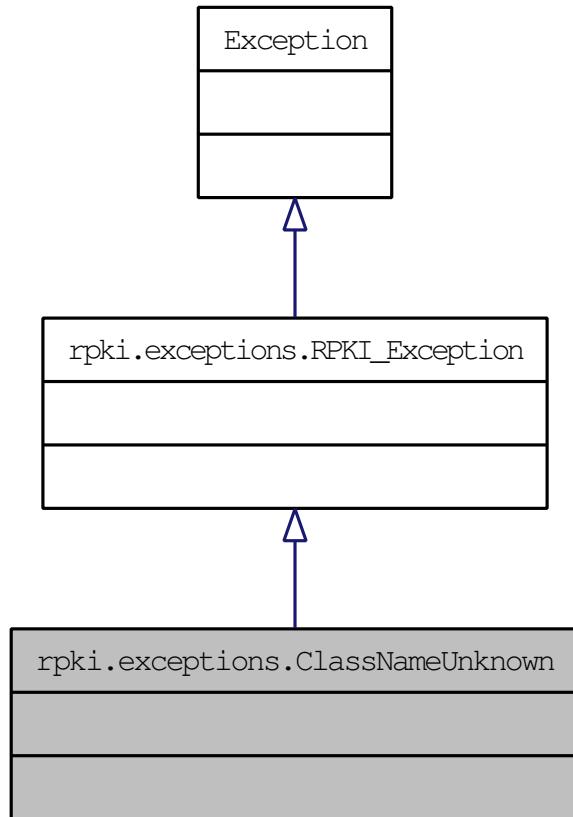
The documentation for this class was generated from the following file:

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

## 11.64 rpki.exceptions.ClassNameUnknown Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpkி.exceptions.ClassNameUnknown:



#### 11.64.1 Detailed Description

Unknown class\_name.

Definition at line 137 of file exceptions.py.

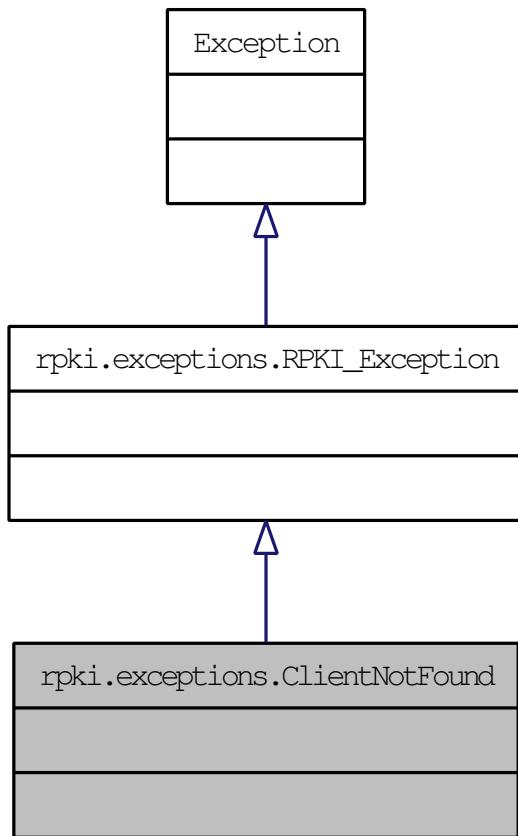
The documentation for this class was generated from the following file:

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

## 11.65 rpkி.exceptions.ClientNotFound Class Reference

Inherits [rpkி::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpkி.exceptions.ClientNotFound:



### 11.65.1 Detailed Description

Could not find specified client in database.

Definition at line 237 of file exceptions.py.

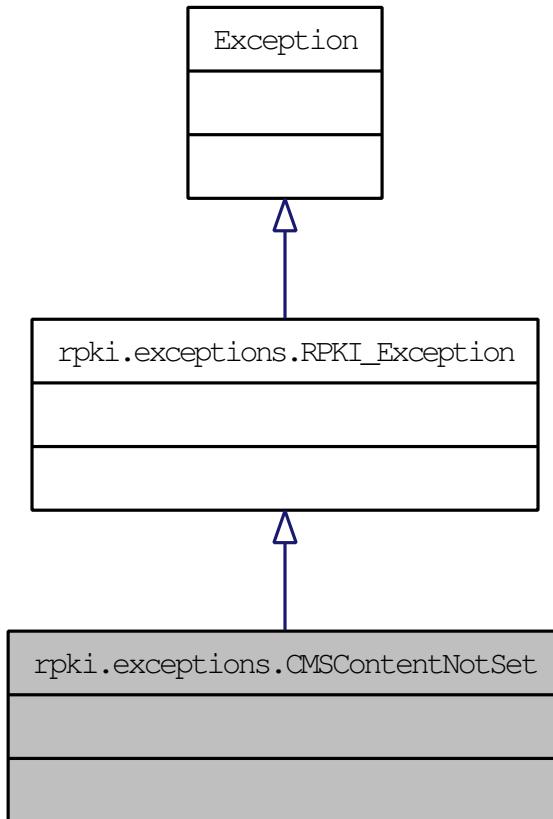
The documentation for this class was generated from the following file:

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

## 11.66 rpkி.exceptions.CMSContentNotSet Class Reference

Inherits [rpkième.exceptions.RPKI\\_Exception](#).

Collaboration diagram for rpkி.exceptions.CMSContentNotSet:



### 11.66.1 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.

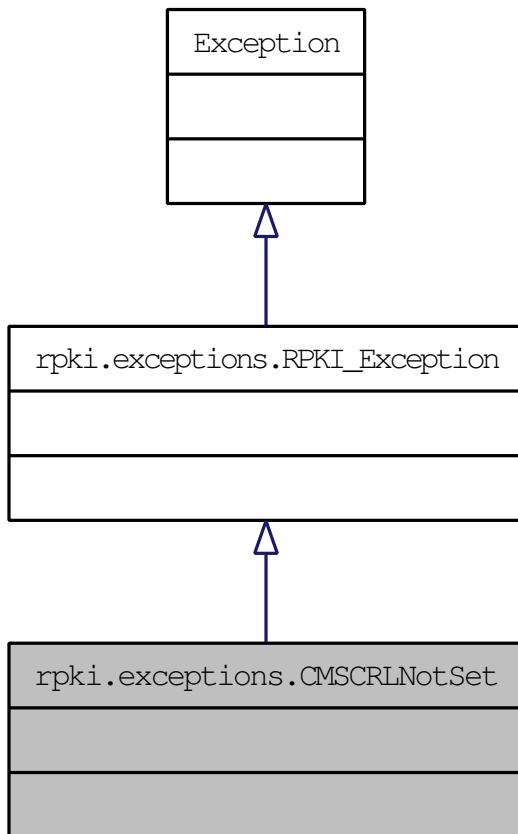
The documentation for this class was generated from the following file:

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

## 11.67 rpkி.exceptions.CMSCRLNotSet Class Reference

Inherits [rpkி::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpkி.exceptions.CMSCRLNotSet:



### 11.67.1 Detailed Description

CMS CRL has not been configured.

Definition at line 217 of file exceptions.py.

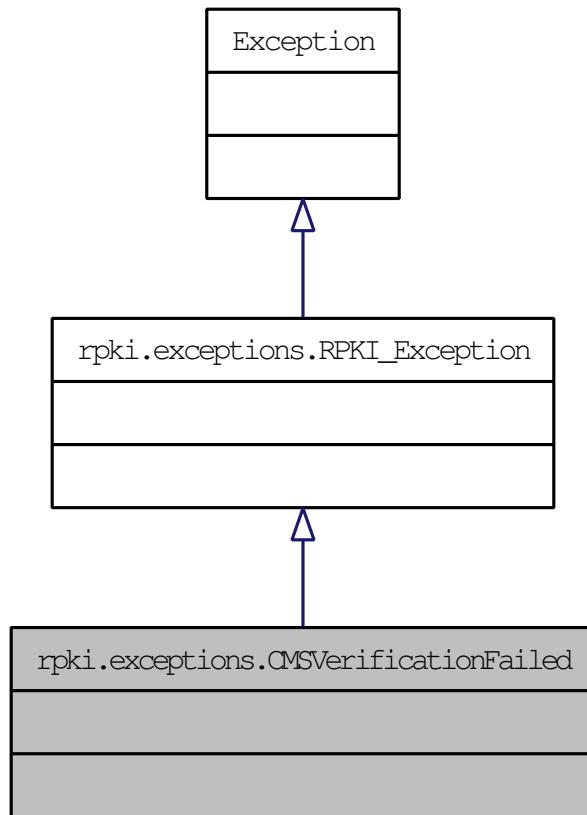
The documentation for this class was generated from the following file:

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

## 11.68 rpki.exceptions.CMSVerificationFailed Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.CMSVerificationFailed:



### 11.68.1 Detailed Description

Verification of a CMS message failed.

Definition at line 66 of file exceptions.py.

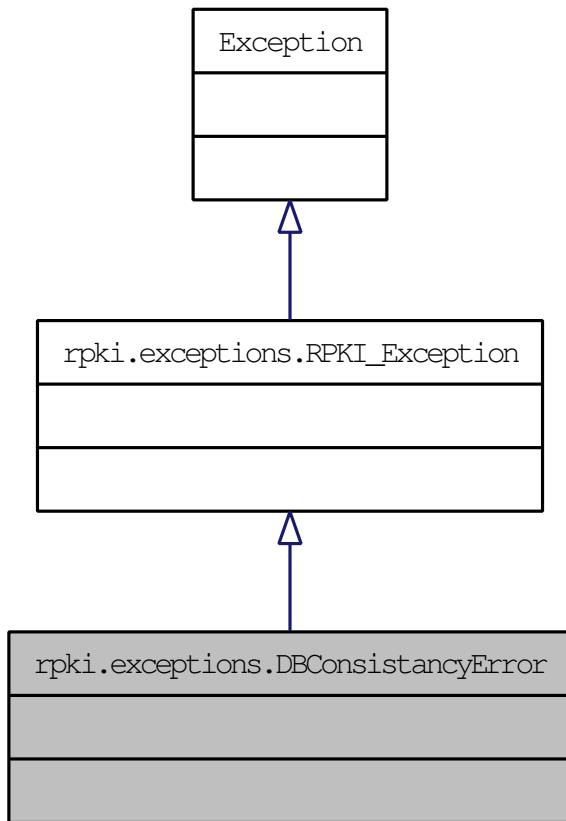
The documentation for this class was generated from the following file:

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

## 11.69 rpki.exceptions.DBConsistencyError Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.DBConsistencyError:



### 11.69.1 Detailed Description

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

Definition at line 60 of file exceptions.py.

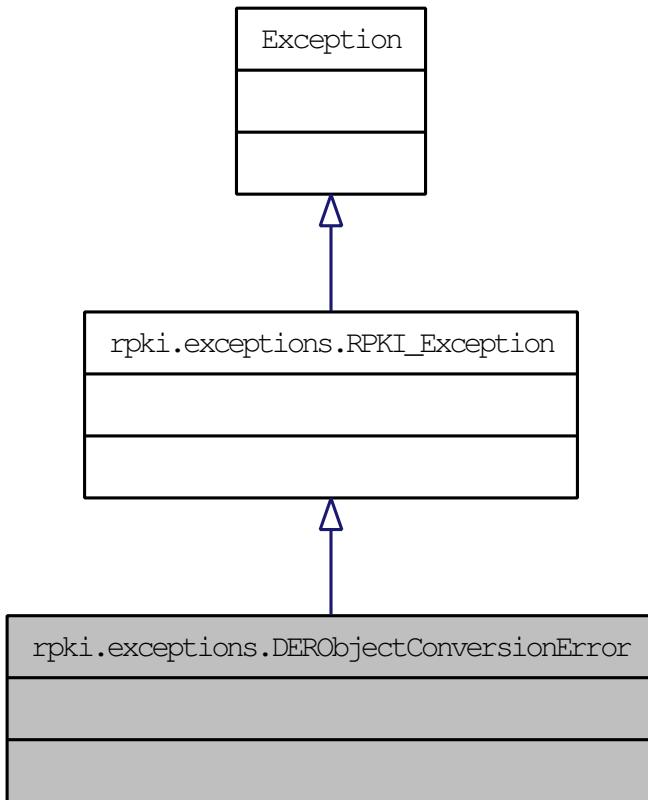
The documentation for this class was generated from the following file:

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

## 11.70 rpkி.exceptions.DERObjectConversionError Class Reference

Inherits [rpkி::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpkி.exceptions.DERObjectConversionError:



### 11.70.1 Detailed Description

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

Definition at line 76 of file `exceptions.py`.

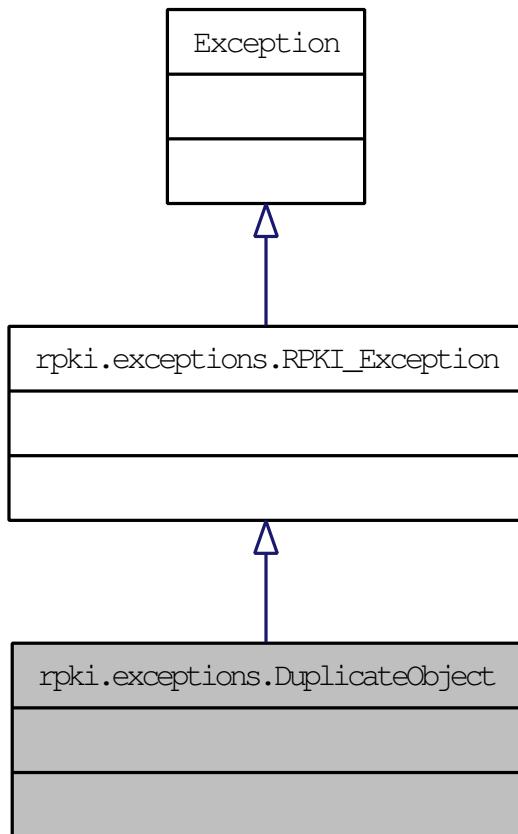
The documentation for this class was generated from the following file:

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

## 11.71 rpki.exceptions.DuplicateObject Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.DuplicateObject:



### 11.71.1 Detailed Description

Attempt to create an object that already exists.

Definition at line 262 of file exceptions.py.

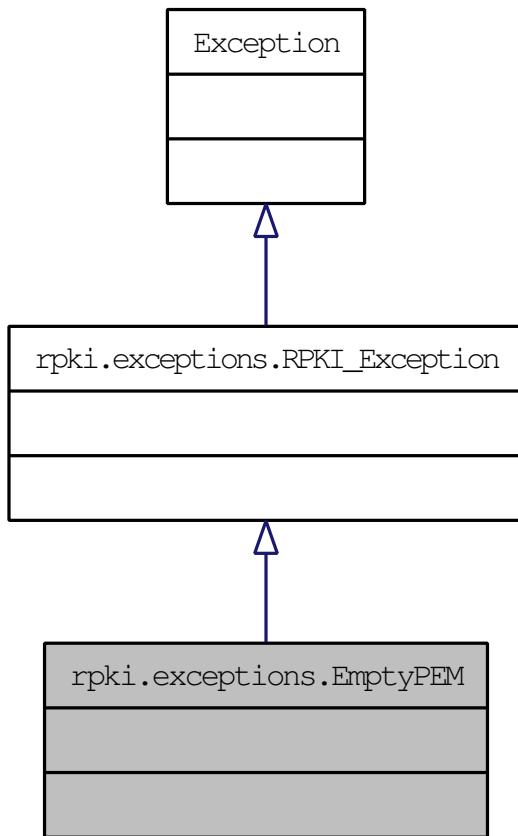
The documentation for this class was generated from the following file:

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

## 11.72 rpki.exceptions.EmptyPEM Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.EmptyPEM:



### 11.72.1 Detailed Description

Couldn't find PEM block to convert.

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

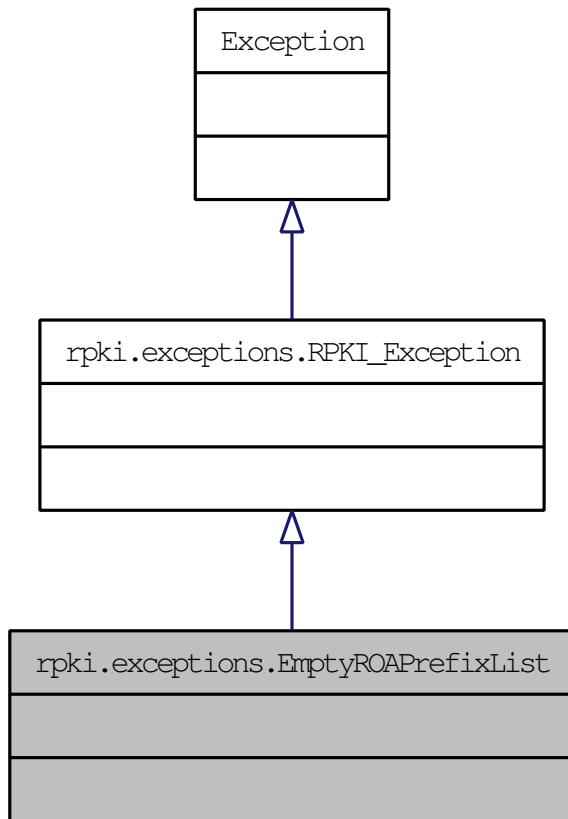
The documentation for this class was generated from the following file:

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

## 11.73 rpki.exceptions.EmptyROAPrefixList Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.EmptyROAPrefixList:



### 11.73.1 Detailed Description

Can't create ROA with an empty prefix list.

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

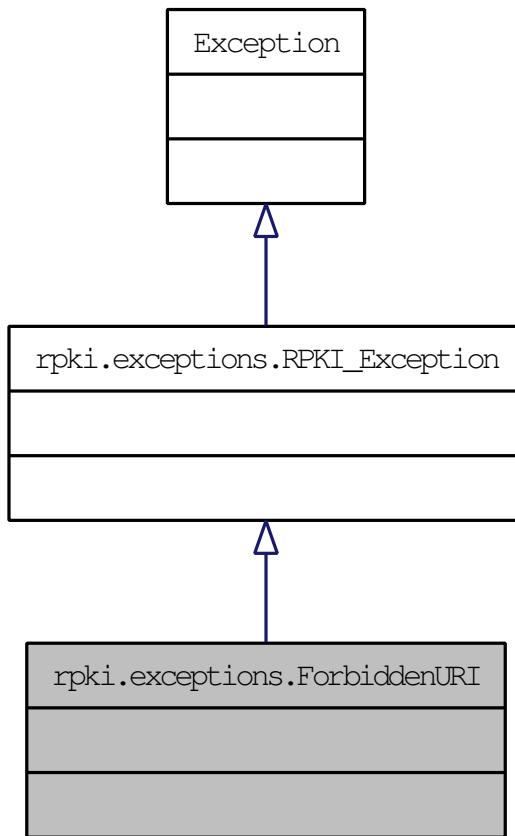
The documentation for this class was generated from the following file:

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

## 11.74 rpki.exceptions.ForbiddenURI Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.ForbiddenURI:



### 11.74.1 Detailed Description

Forbidden URI, does not start with correct base URI.

Definition at line 247 of file exceptions.py.

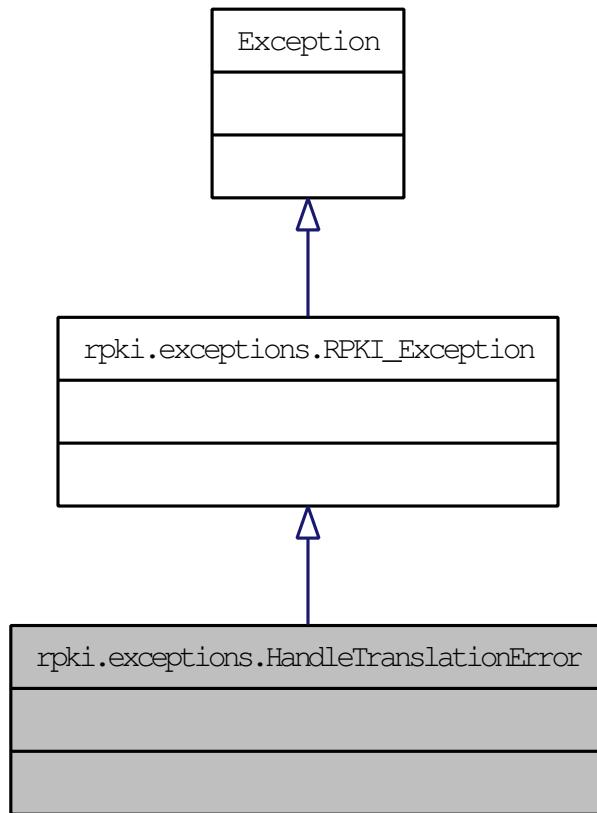
The documentation for this class was generated from the following file:

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

## 11.75 rpki.exceptions.HandleTranslationError Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.HandleTranslationError:



### 11.75.1 Detailed Description

Internal error translating protocol handle -> SQL id.

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

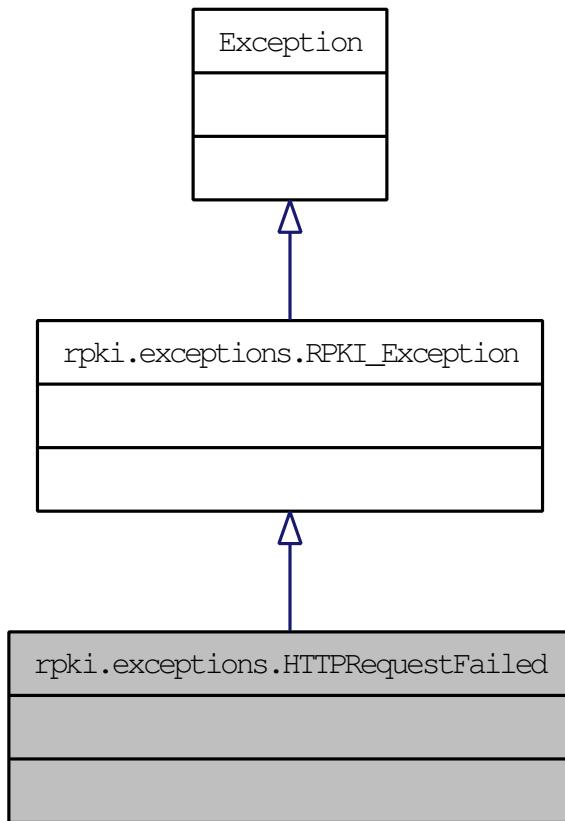
The documentation for this class was generated from the following file:

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

## 11.76 rpkி.exceptions.HTTPRequestFailed Class Reference

Inherits [rpkி::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpkி.exceptions.HTTPRequestFailed:



### 11.76.1 Detailed Description

HTTP request failed.

Definition at line 71 of file exceptions.py.

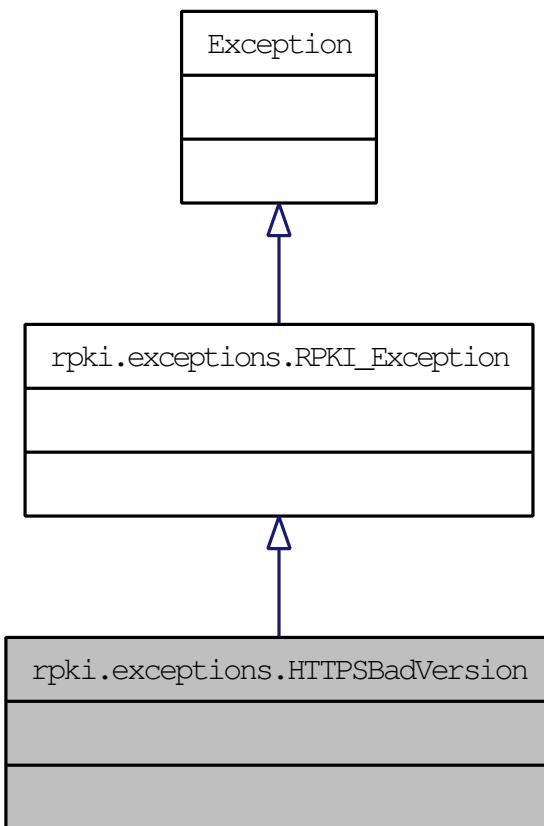
The documentation for this class was generated from the following file:

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

## 11.77 rpkி.exceptions.HTTPSBadVersion Class Reference

Inherits [rpkி::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpkி.exceptions.HTTPSBadVersion:



### 11.77.1 Detailed Description

HTTPS couldn't parse HTTP version.

Definition at line 287 of file exceptions.py.

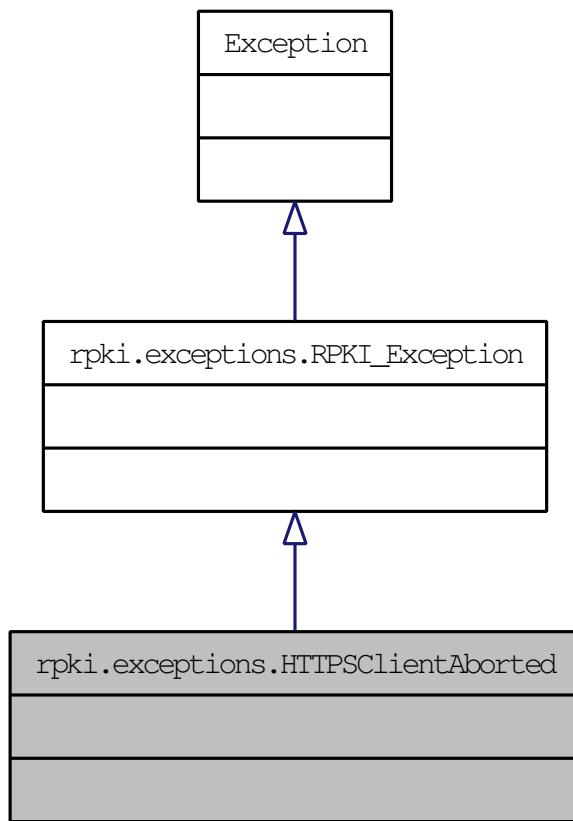
The documentation for this class was generated from the following file:

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

## 11.78 rpki.exceptions.HTTPSClientAborted Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.HTTPSClientAborted:



### 11.78.1 Detailed Description

HTTPS client connection closed while in request-sent state.

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

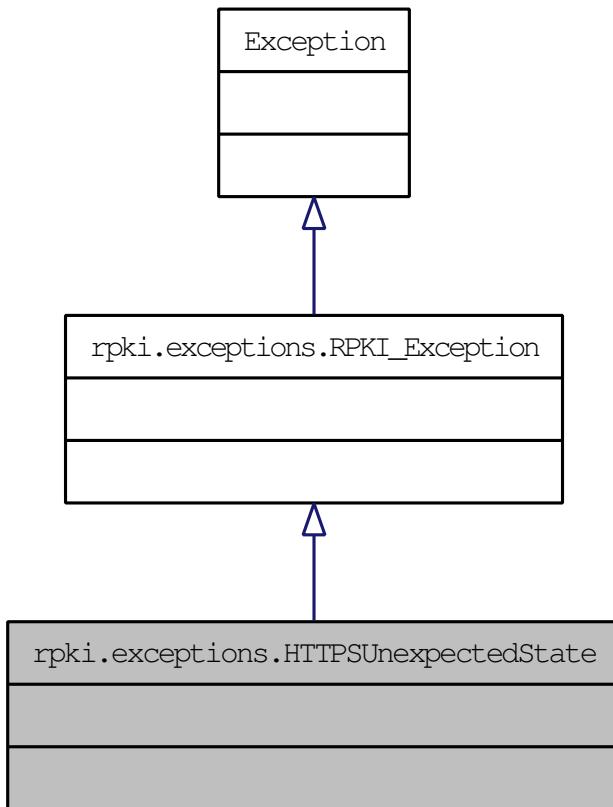
The documentation for this class was generated from the following file:

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

## 11.79 rpki.exceptions.HTTPSUnexpectedState Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.HTTPSUnexpectedState:



### 11.79.1 Detailed Description

HTTPS event occurred in an unexpected state.

Definition at line 282 of file exceptions.py.

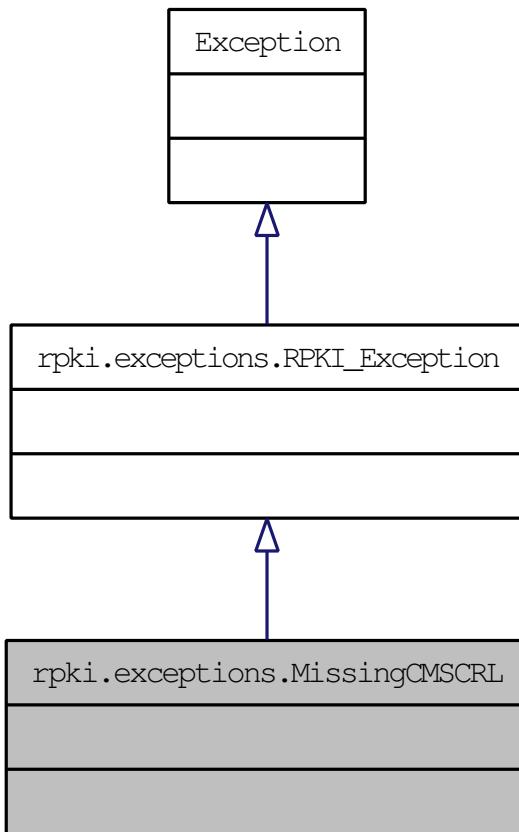
The documentation for this class was generated from the following file:

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

## 11.80 rpki.exceptions.MissingCMSCRL Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.MissingCMSCRL:



### 11.80.1 Detailed Description

Didn't receive CMS CRL when expecting one.

Definition at line 207 of file `exceptions.py`.

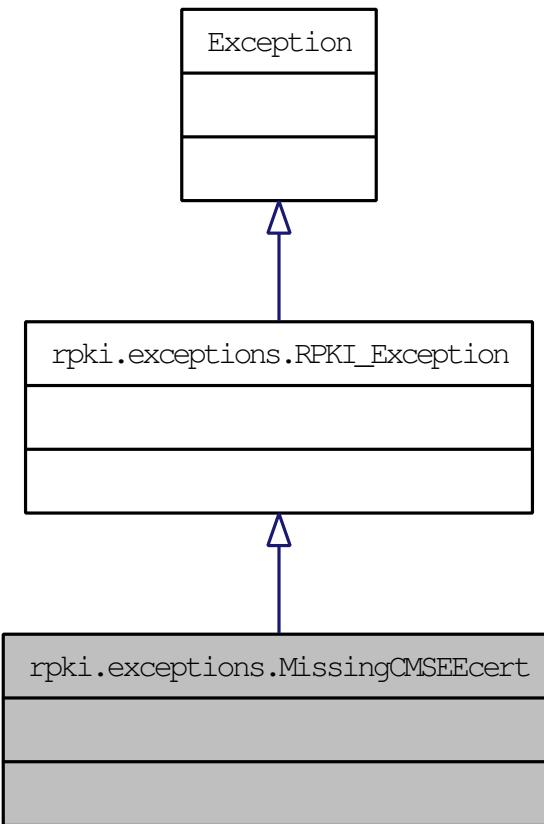
The documentation for this class was generated from the following file:

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

## 11.81 rpkி.exceptions.MissingCMSEEcrt Class Reference

Inherits [rpkி::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpkி.exceptions.MissingCMSEEcrt:



### 11.81.1 Detailed Description

Didn't receive CMS EE cert when expecting one.

Definition at line 202 of file exceptions.py.

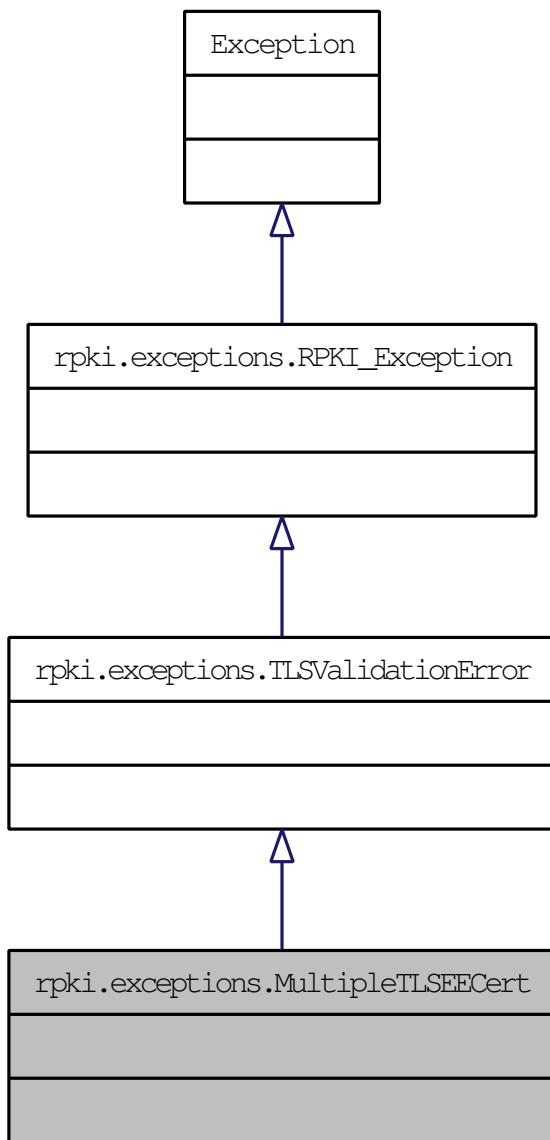
The documentation for this class was generated from the following file:

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

## 11.82 rpki.exceptions.MultipleTLSEECert Class Reference

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

Collaboration diagram for rpki.exceptions.MultipleTLSEECert:



### 11.82.1 Detailed Description

Received more than one TLS EE certificate.

Definition at line 172 of file exceptions.py.

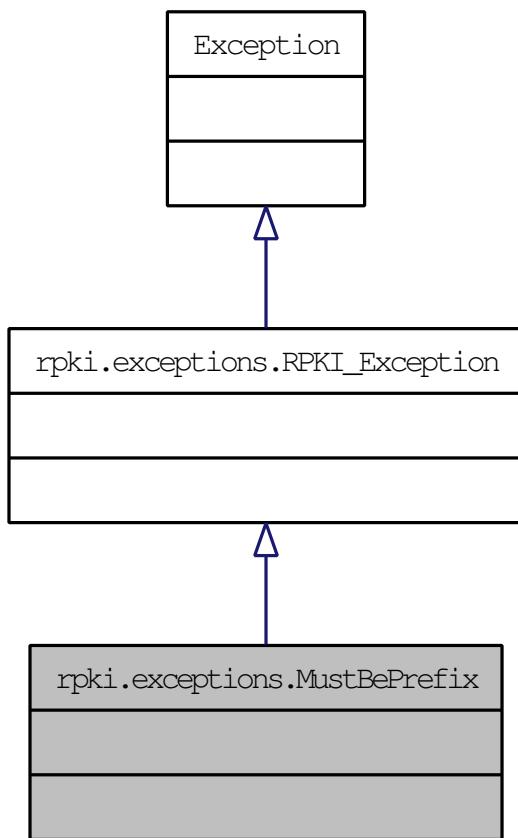
The documentation for this class was generated from the following file:

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

## 11.83 rpki.exceptions.MustBePrefix Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.MustBePrefix:



### 11.83.1 Detailed Description

Resource range cannot be expressed as a prefix.

Definition at line 162 of file exceptions.py.

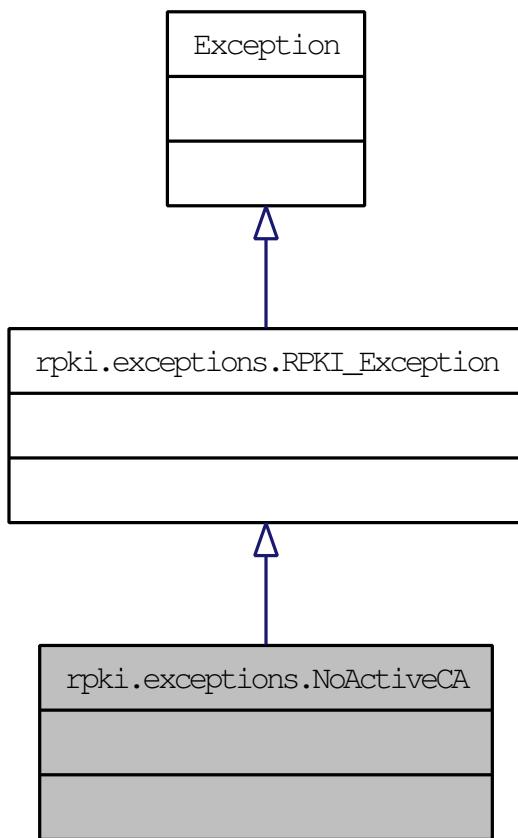
The documentation for this class was generated from the following file:

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

## 11.84 rpki.exceptions.NoActiveCA Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.NoActiveCA:



### 11.84.1 Detailed Description

No active ca\_detail for specified class.

Definition at line 227 of file exceptions.py.

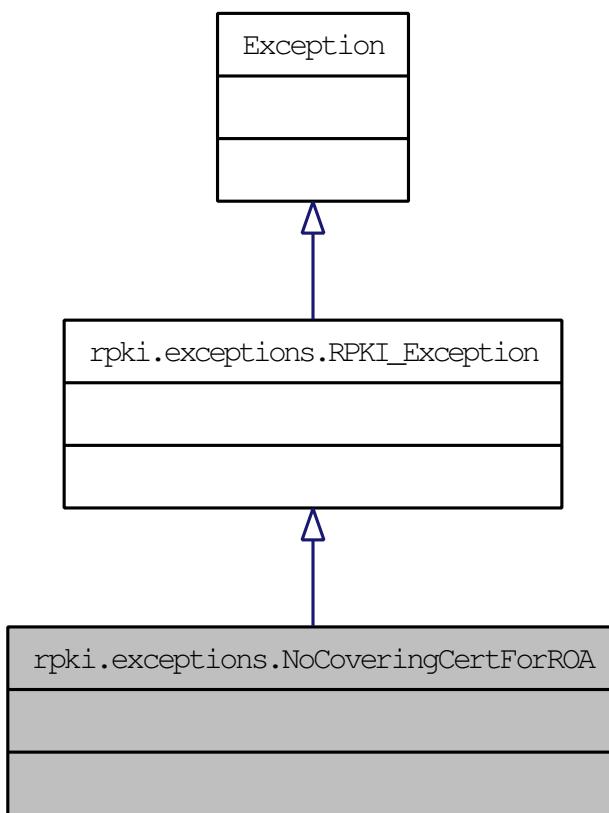
The documentation for this class was generated from the following file:

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

## 11.85 rpki.exceptions.NoCoveringCertForROA Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.NoCoveringCertForROA:



### 11.85.1 Detailed Description

Couldn't find a covering certificate to generate ROA.

Definition at line 272 of file exceptions.py.

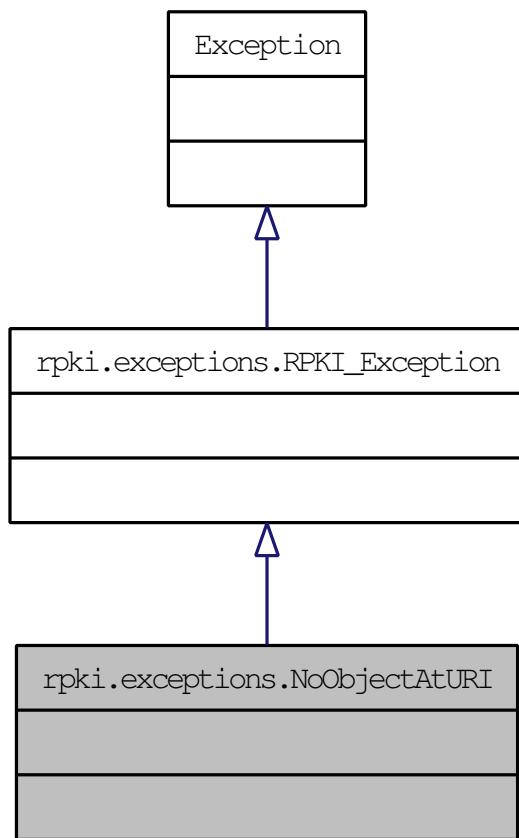
The documentation for this class was generated from the following file:

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

## 11.86 rpki.exceptions.NoObjectAtURI Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.NoObjectAtURI:



### 11.86.1 Detailed Description

No object published at specified URI.

Definition at line 297 of file exceptions.py.

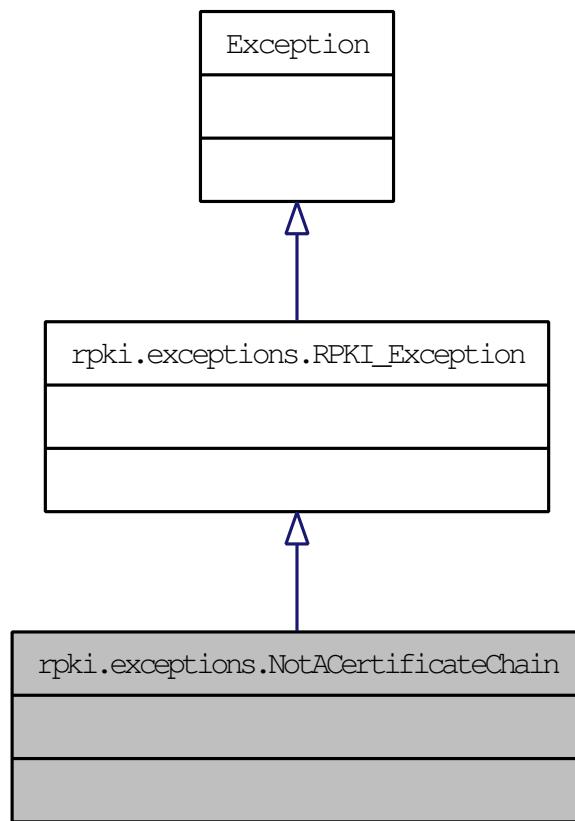
The documentation for this class was generated from the following file:

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

## 11.87 rpki.exceptions.NotACertificateChain Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.NotACertificateChain:



### 11.87.1 Detailed Description

Certificates don't form a proper chain.

Definition at line 82 of file exceptions.py.

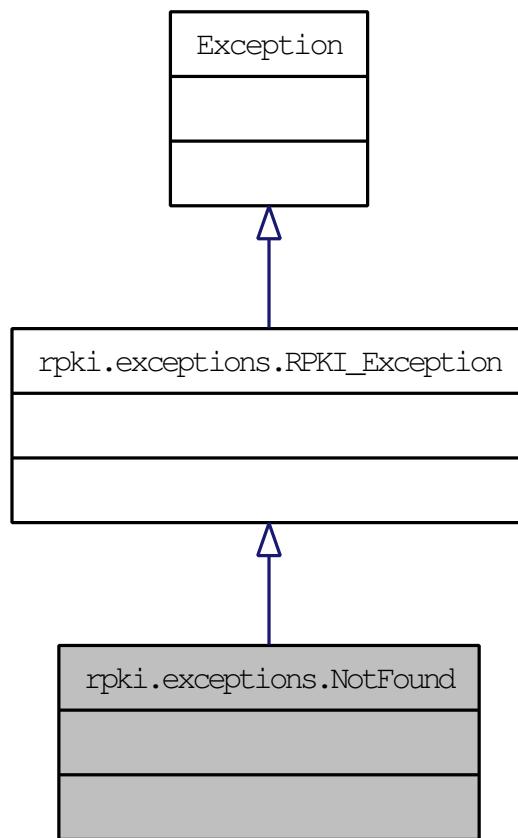
The documentation for this class was generated from the following file:

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

## 11.88 rpki.exceptions.NotFound Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.NotFound:



### 11.88.1 Detailed Description

Object not found in database.

Definition at line 157 of file exceptions.py.

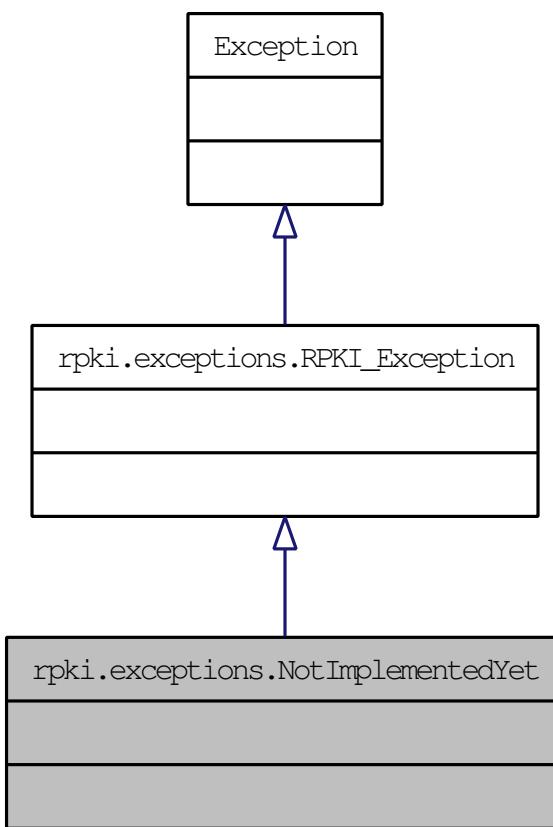
The documentation for this class was generated from the following file:

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

## 11.89 rpki.exceptions.NotImplementedYet Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.NotImplementedYet:



### 11.89.1 Detailed Description

Internal error -- not implemented yet.

Definition at line 102 of file exceptions.py.

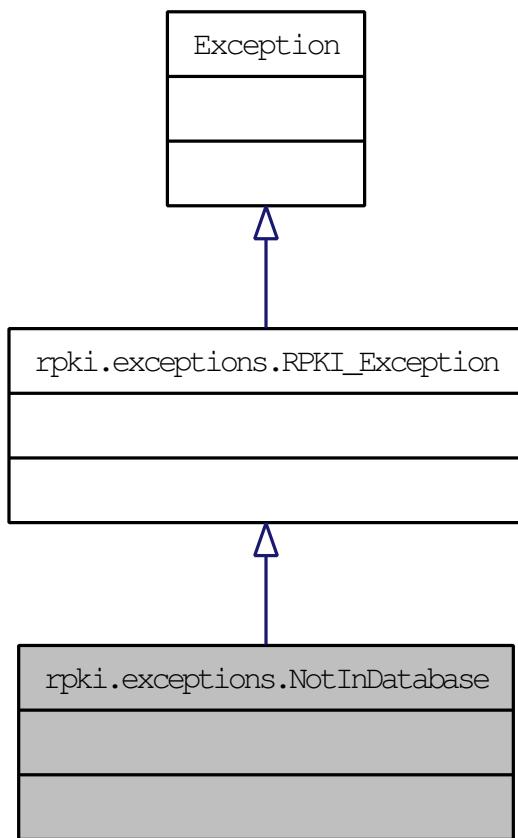
The documentation for this class was generated from the following file:

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

## 11.90 rpki.exceptions.NotInDatabase Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.NotInDatabase:



### 11.90.1 Detailed Description

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

Definition at line 40 of file exceptions.py.

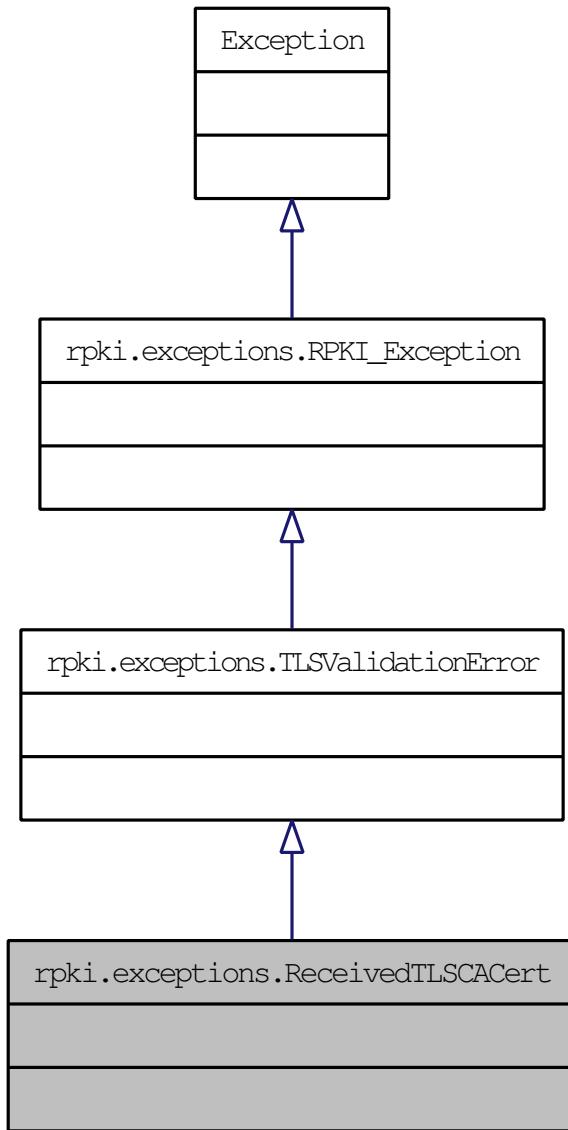
The documentation for this class was generated from the following file:

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

## 11.91 rpki.exceptions.ReceivedTLSCACert Class Reference

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

Collaboration diagram for rpki.exceptions.ReceivedTLSCACert:



### 11.91.1 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:

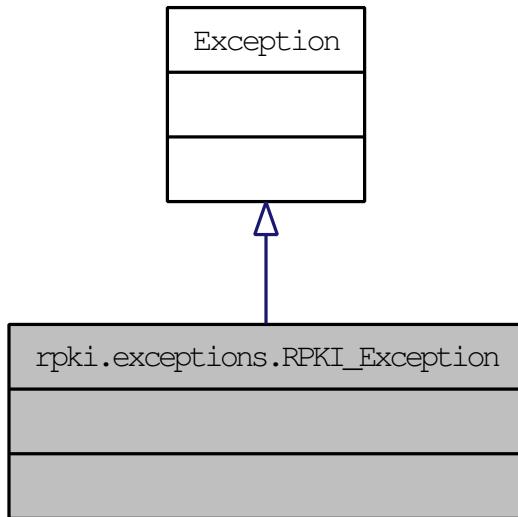
- [exceptions.py \(2907\)](#)

## 11.92 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:



### 11.92.1 Detailed Description

Base class for RPKI exceptions.

Definition at line 35 of file exceptions.py.

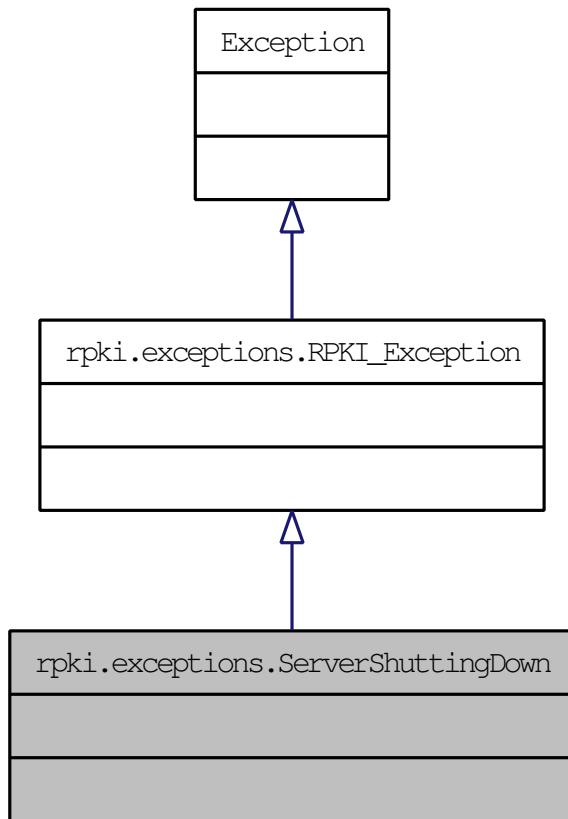
The documentation for this class was generated from the following file:

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

## 11.93 rpki.exceptions.ServerShuttingDown Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpkி.exceptions.ServerShuttingDown:



### 11.93.1 Detailed Description

Server is shutting down.

Definition at line 222 of file exceptions.py.

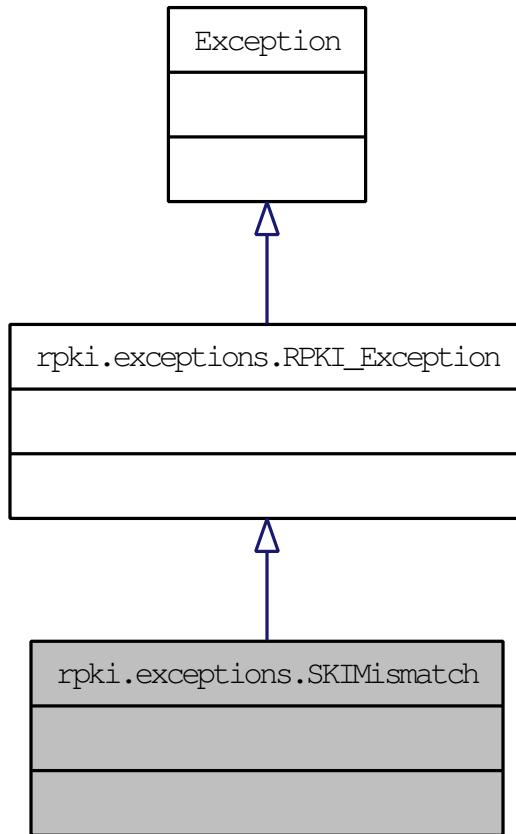
The documentation for this class was generated from the following file:

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

## 11.94 rpkி.exceptions.SKIMismatch Class Reference

Inherits [rpkி::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.SKIMismatch:



#### 11.94.1 Detailed Description

SKI value in response does not match request.

Definition at line 142 of file exceptions.py.

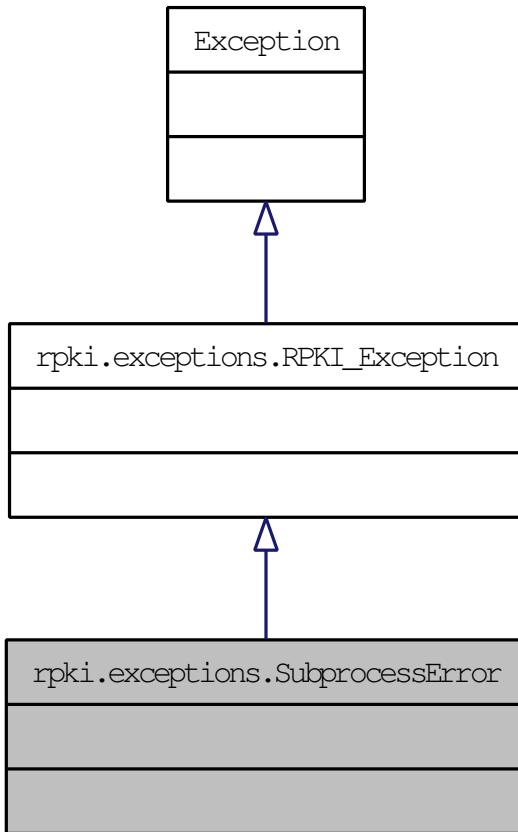
The documentation for this class was generated from the following file:

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

## 11.95 rpki.exceptions.SubprocessError Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.SubprocessError:



### 11.95.1 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:

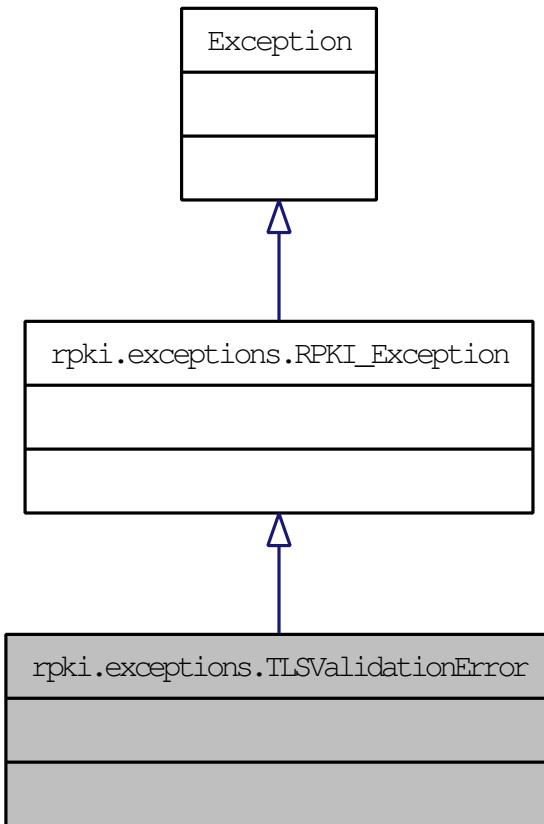
- [exceptions.py \(2907\)](#)

## 11.96 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:



### 11.96.1 Detailed Description

TLS certificate validation error.

Definition at line 167 of file exceptions.py.

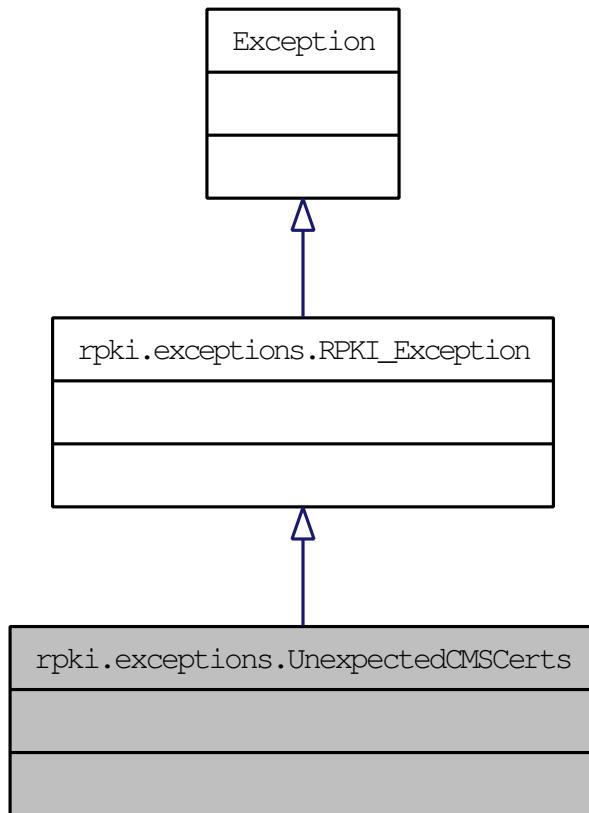
The documentation for this class was generated from the following file:

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

## 11.97 rpkி.exceptions.UnexpectedCMSCerts Class Reference

Inherits [rpkி::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpkி.exceptions.UnexpectedCMSCerts:



### 11.97.1 Detailed Description

Received CMS certs when not expecting any.

Definition at line 192 of file exceptions.py.

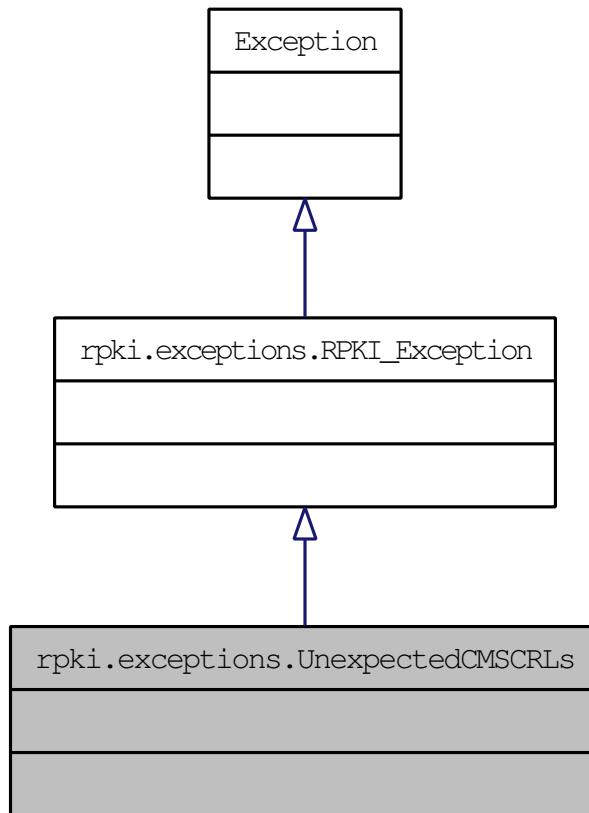
The documentation for this class was generated from the following file:

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

## 11.98 rpki.exceptions.UnexpectedCMSCRLs Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.UnexpectedCMSCRLs:



### 11.98.1 Detailed Description

Received CMS CRLs when not expecting any.

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

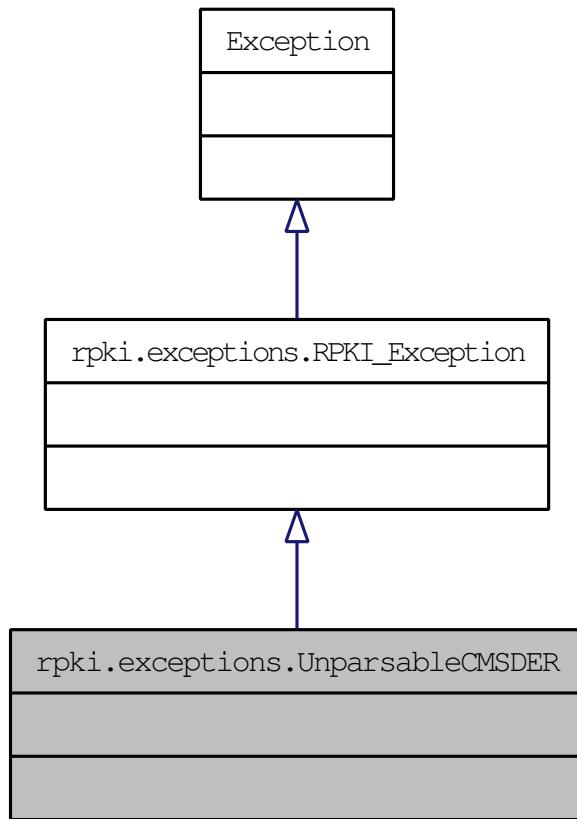
The documentation for this class was generated from the following file:

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

## 11.99 rpki.exceptions.UnparsableCMDSER Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.UnparsableCMDSER:



### 11.99.1 Detailed Description

Alleged CMS DER wasn't parsable.

Definition at line 212 of file exceptions.py.

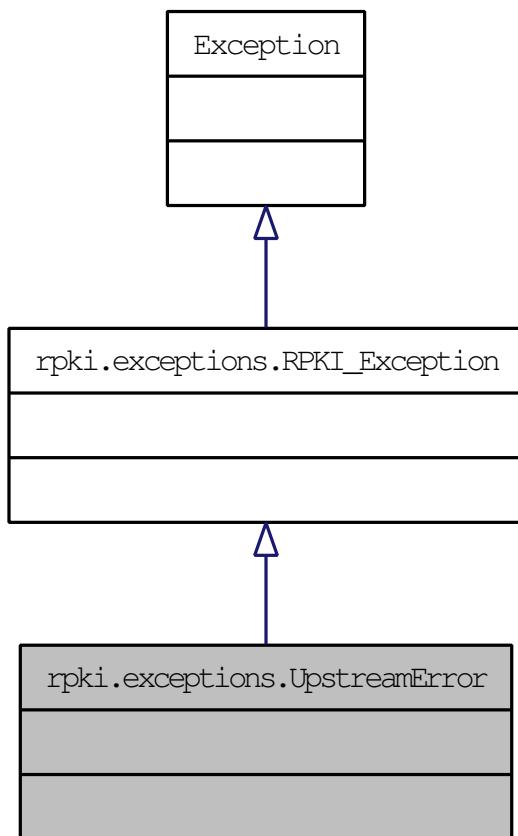
The documentation for this class was generated from the following file:

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

## 11.100 rpki.exceptions.UpstreamError Class Reference

Inherits [rpki::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpki.exceptions.UpstreamError:



### 11.100.1 Detailed Description

Received an error from upstream.

Definition at line 112 of file `exceptions.py`.

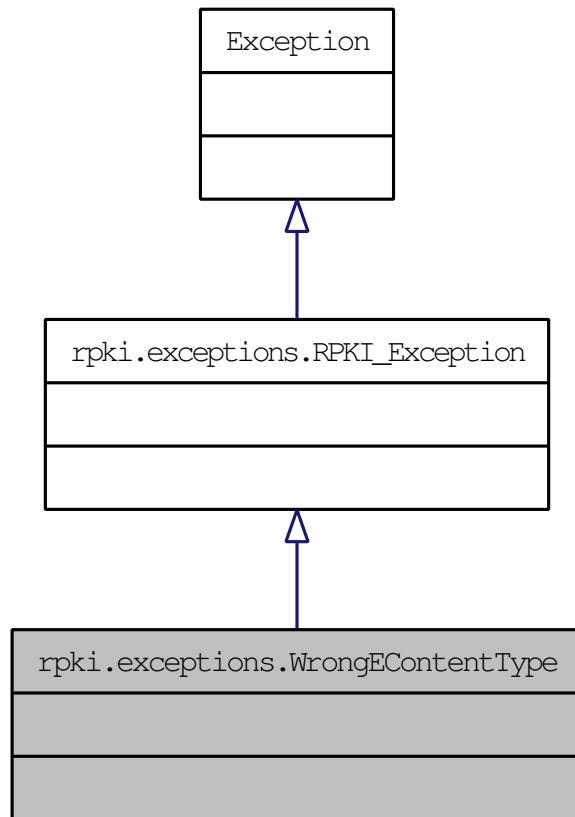
The documentation for this class was generated from the following file:

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

## 11.101 rpkி.exceptions.WrongEContentType Class Reference

Inherits [rpkி::exceptions::RPKI\\_Exception](#).

Collaboration diagram for rpkி.exceptions.WrongEContentType:



### 11.101.1 Detailed Description

Received wrong CMS eContentType.

Definition at line 182 of file exceptions.py.

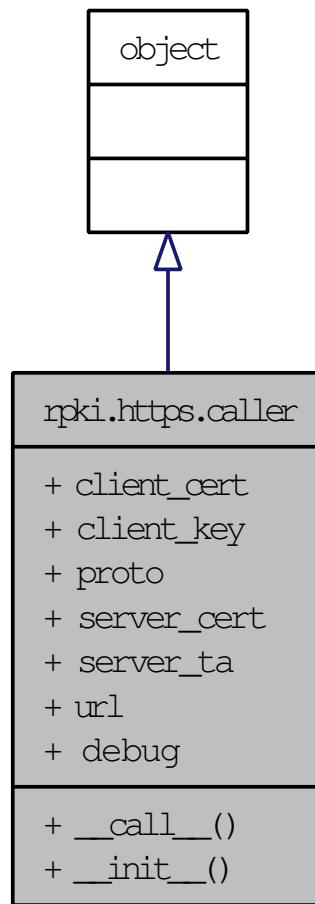
The documentation for this class was generated from the following file:

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

## 11.102 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

### 11.102.1 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.

### 11.102.2 Member Function Documentation

#### 11.102.2.1 def rpkি.https.caller.\_\_call\_\_ ( *self*, *cb*, *eb*, *pdu*s )

Definition at line 1124 of file https.py.

#### 11.102.2.2 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.

### 11.102.3 Member Data Documentation

#### 11.102.3.1 rpkি.https.caller.client\_cert

Definition at line 1117 of file https.py.

**11.102.3.2 rpki.https.caller.client\_key**

Definition at line 1116 of file https.py.

**11.102.3.3 rpki.https.caller.debug = False [static]**

Definition at line 1112 of file https.py.

**11.102.3.4 rpki.https.caller.proto**

Definition at line 1115 of file https.py.

**11.102.3.5 rpki.https.caller.server\_cert**

Definition at line 1119 of file https.py.

**11.102.3.6 rpki.https.caller.server\_ta**

Definition at line 1118 of file https.py.

**11.102.3.7 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 \(3191\)](#)

**11.103 rpki.https.http\_client Class Reference**

Inherits [rpki::https::http\\_stream](#).

Collaboration diagram for rpki.https.http\_client:



## Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [handle\\_close](#)
- def [handle\\_connect](#)
- def [handle\\_error](#)
- def [handle\\_message](#)

- def `handle_no_content_length`
- def `handle_timeout`
- def `send_request`
- def `set_state`
- def `start`
- def `tls_connect`

### Public Attributes

- `af`
- `cert`
- `expect_close`
- `hostport`
- `key`
- `queue`
- `retry_read`
- `retry_write`
- `state`
- `ta`
- `tls`

### Static Public Attributes

- `parse_type = http_response`  
*Stream parser should look for incoming HTTP response messages.*

- `timeout = default_client_timeout`  
*Use the default client timeout value set in the module header.*

### 11.103.1 Detailed Description

HTTP (S) client stream.

Definition at line 759 of file https.py.

### 11.103.2 Member Function Documentation

#### 11.103.2.1 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.

**11.103.2.2 def rpkি.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 [rpkি.https.http\\_stream](#).

Definition at line 892 of file https.py.

**11.103.2.3 def rpkি.https.http\_client.handle\_connect (*self*)**

Asyncore says socket has connected, configure TLS junk.

Definition at line 797 of file https.py.

**11.103.2.4 def rpkি.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 [rpkি.https.http\\_stream](#).

Definition at line 918 of file https.py.

**11.103.2.5 def rpkি.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.

**11.103.2.6 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.

**11.103.2.7 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.

**11.103.2.8 def rpki.https.http\_client.send\_request ( *self*, *msg* )**

Queue up request message and kickstart connection.

Definition at line 845 of file https.py.

**11.103.2.9 def rpki.https.http\_client.set\_state ( *self*, *state* )**

Set HTTP client connection state.

Definition at line 829 of file https.py.

**11.103.2.10 def rpki.https.http\_client.start ( *self* )**

Create socket and request a connection.

Definition at line 785 of file https.py.

**11.103.2.11 def rpki.https.http\_client.tls\_connect (*self*)**

Initialize client side of TLS.

Definition at line 814 of file https.py.

**11.103.3 Member Data Documentation****11.103.3.1 rpki.https.http\_client.af**

Definition at line 783 of file https.py.

**11.103.3.2 rpki.https.http\_client.cert**

Definition at line 780 of file https.py.

**11.103.3.3 rpki.https.http\_client.expect\_close**

Definition at line 779 of file https.py.

**11.103.3.4 rpki.https.http\_client.hostport**

Definition at line 777 of file https.py.

**11.103.3.5 rpki.https.http\_client.key**

Definition at line 781 of file https.py.

**11.103.3.6 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.

#### 11.103.3.7 rpki.https.http\_client.queue

Definition at line 776 of file https.py.

#### 11.103.3.8 rpki.https.http\_client.retry\_read

Reimplemented from [rpki.https.http\\_stream](#).

Definition at line 821 of file https.py.

#### 11.103.3.9 rpki.https.http\_client.retry\_write

Reimplemented from [rpki.https.http\\_stream](#).

Definition at line 823 of file https.py.

#### 11.103.3.10 rpki.https.http\_client.state

Definition at line 778 of file https.py.

#### 11.103.3.11 rpki.https.http\_client.ta

Definition at line 782 of file https.py.

#### 11.103.3.12 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.

### 11.103.3.13 rpki.https.http\_client.tls

Reimplemented from [rpki.https.http\\_stream](#).

Definition at line 802 of file https.py.

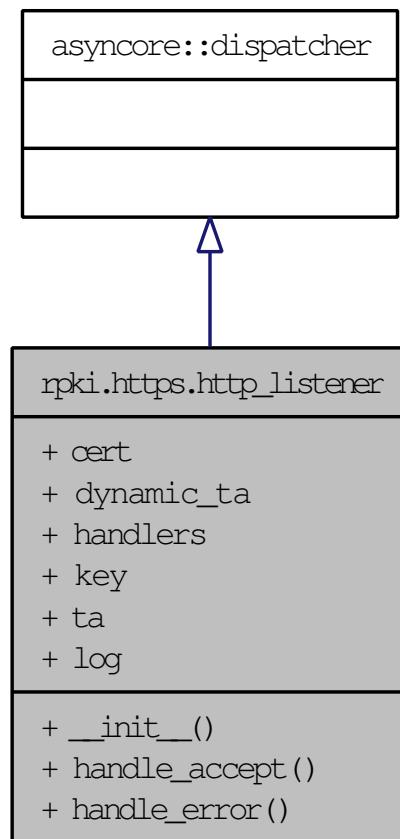
The documentation for this class was generated from the following file:

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

## 11.104 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

### 11.104.1 Detailed Description

Listener for incoming HTTP(S) connections.

Definition at line 707 of file https.py.

### 11.104.2 Member Function Documentation

#### 11.104.2.1 def rpkি.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.

#### 11.104.2.2 def rpkি.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.

**11.104.2.3 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.

**11.104.3 Member Data Documentation****11.104.3.1 rpki.https.http\_listener.cert**

Definition at line 718 of file https.py.

**11.104.3.2 rpki.https.http\_listener.dynamic\_ta**

Definition at line 721 of file https.py.

**11.104.3.3 rpki.https.http\_listener.handlers**

Definition at line 717 of file https.py.

**11.104.3.4 rpki.https.http\_listener.key**

Definition at line 719 of file https.py.

**11.104.3.5 rpki.https.http\_listener.log = log\_method [static]**

Definition at line 712 of file https.py.

**11.104.3.6 rpki.https.http\_listener.ta**

Definition at line 720 of file https.py.

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

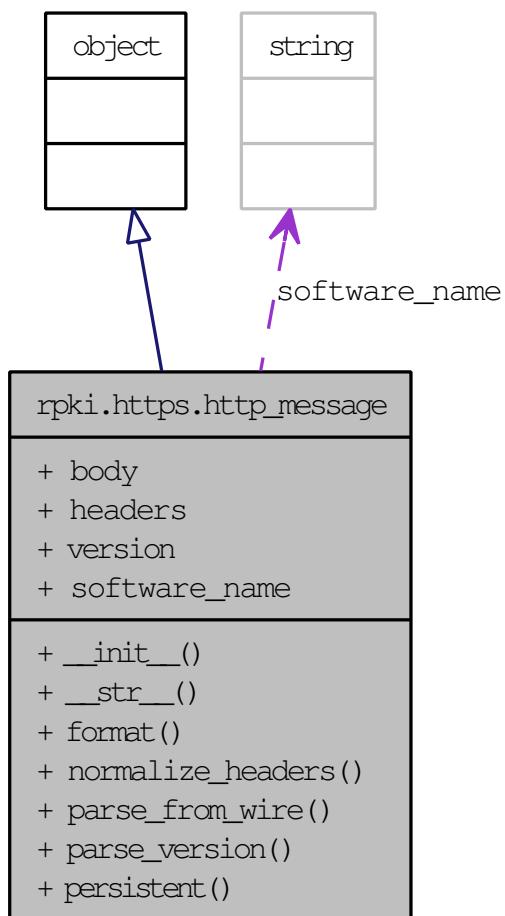
- [https.py \(3191\)](#)

## 11.105 rpkি.https.http\_message Class Reference

Inherits [object](#).

Inherited by [rpkি.https.http\\_request](#), and [rpkি.https.http\\_response](#).

Collaboration diagram for rpkি.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"

#### 11.105.1 Detailed Description

Virtual class representing of one HTTP message.

Definition at line 90 of file https.py.

#### 11.105.2 Member Function Documentation

##### 11.105.2.1 def rpkি.https.http\_message.\_\_init\_\_(*self*, *version* = **None**, *body* = **None**, *headers* = **None**)

Definition at line 97 of file https.py.

##### 11.105.2.2 def rpkি.https.http\_message.\_\_str\_\_(*self*)

Definition at line 155 of file https.py.

**11.105.2.3 def rpkি.https.http\_message.format (*self*)**

Format an outgoing HTTP message.

Definition at line 140 of file https.py.

**11.105.2.4 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.

**11.105.2.5 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.

**11.105.2.6 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.

**11.105.2.7 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.

**11.105.3 Member Data Documentation****11.105.3.1 rpki.https.http\_message.body**

Definition at line 99 of file https.py.

**11.105.3.2 rpki.https.http\_message.headers**

Definition at line 100 of file https.py.

**11.105.3.3 string rpki.https.http\_message.software\_name = "ISC RPKI library" [static]**

Definition at line 95 of file https.py.

**11.105.3.4 rpki.https.http\_message.version**

Definition at line 98 of file https.py.

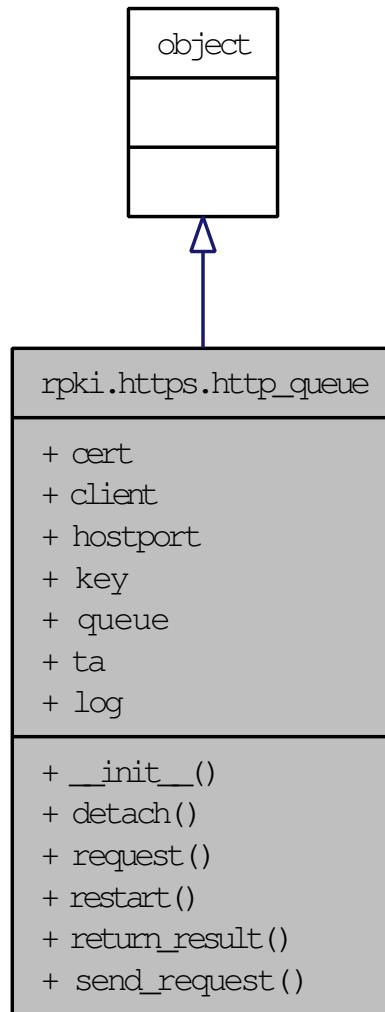
The documentation for this class was generated from the following file:

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

**11.106 rpki.https.http\_queue Class Reference**

Inherits [object](#).

Collaboration diagram for rPKI.https.http\_queue:



### Public Member Functions

- def `__init__`
- def `detach`
- def `request`
- def `restart`
- def `return_result`
- def `send_request`

## Public Attributes

- [cert](#)
- [client](#)
- [hostport](#)
- [key](#)
- [queue](#)
- [ta](#)

## Static Public Attributes

- [log](#) = log\_method

### 11.106.1 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.

### 11.106.2 Member Function Documentation

#### 11.106.2.1 def rpkি.https.http\_queue.\_\_init\_\_ ( self, hostport, cert = None, key = None, ta = () )

Definition at line 938 of file https.py.

#### 11.106.2.2 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.

**11.106.2.3 def rpkি.https.http\_queue.request (*self*, *requests*)**

Append http\_request object(s) to this queue.

Definition at line 948 of file https.py.

**11.106.2.4 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.

**11.106.2.5 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.

**11.106.2.6 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.

**11.106.3 Member Data Documentation****11.106.3.1 rpkি.https.http\_queue.cert**

Definition at line 944 of file https.py.

**11.106.3.2 rpki.https.http\_queue.client**

Definition at line 942 of file https.py.

**11.106.3.3 rpki.https.http\_queue.hostport**

Definition at line 941 of file https.py.

**11.106.3.4 rpki.https.http\_queue.key**

Definition at line 945 of file https.py.

**11.106.3.5 rpki.https.http\_queue.log = log\_method [static]**

Definition at line 936 of file https.py.

**11.106.3.6 rpki.https.http\_queue.queue**

Definition at line 943 of file https.py.

**11.106.3.7 rpki.https.http\_queue.ta**

Definition at line 946 of file https.py.

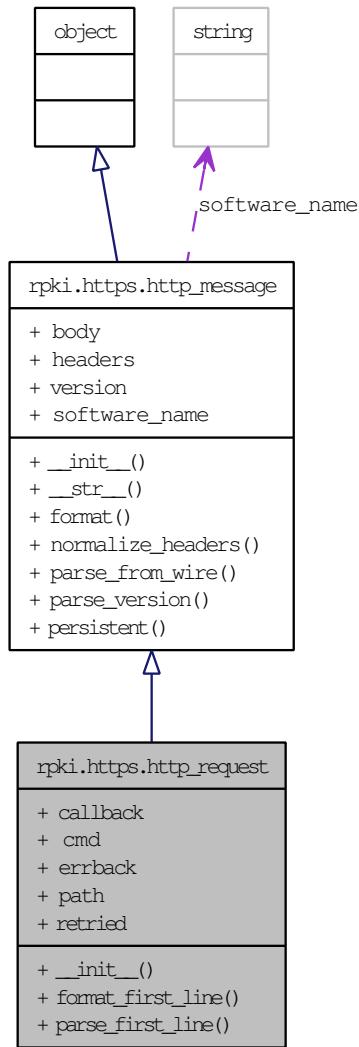
The documentation for this class was generated from the following file:

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

**11.107 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](#)

### 11.107.1 Detailed Description

HTTP request message.

Definition at line 178 of file https.py.

### 11.107.2 Member Function Documentation

#### 11.107.2.1 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.

#### 11.107.2.2 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.

#### 11.107.2.3 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.

**11.107.3 Member Data Documentation****11.107.3.1 rpki.https.http\_request.callback**

Definition at line 188 of file https.py.

**11.107.3.2 rpki.https.http\_request.cmd**

Definition at line 186 of file https.py.

**11.107.3.3 rpki.https.http\_request.errback**

Definition at line 189 of file https.py.

**11.107.3.4 rpki.https.http\_request.path**

Definition at line 187 of file https.py.

**11.107.3.5 rpki.https.http\_request.retried**

Definition at line 190 of file https.py.

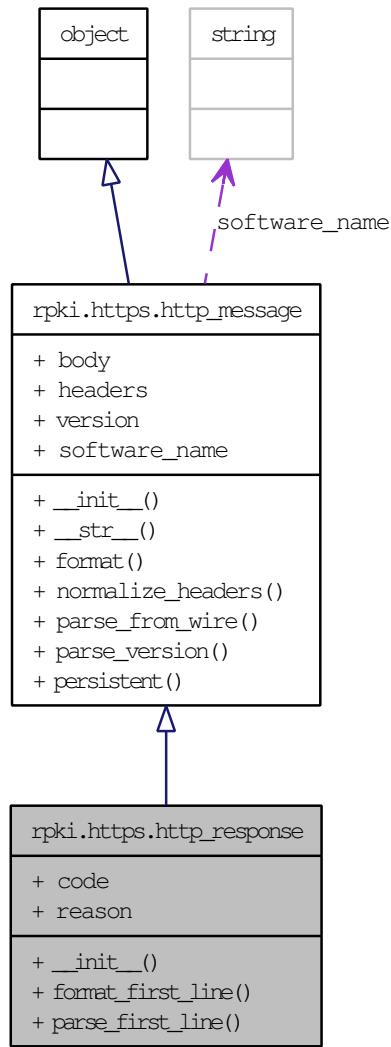
The documentation for this class was generated from the following file:

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

**11.108 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](#)

### 11.108.1 Detailed Description

HTTP response message.

Definition at line 208 of file https.py.

### 11.108.2 Member Function Documentation

#### 11.108.2.1 def rpkি.https.http\_response.\_\_init\_\_ (*self*, *code* = `None`, *reason* = `None`, *version* = `default_http_version`, *body* = `None`, *headers*)

Definition at line 213 of file https.py.

#### 11.108.2.2 def rpkি.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.

#### 11.108.2.3 def rpkি.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.

### 11.108.3 Member Data Documentation

#### 11.108.3.1 rpkি.https.http\_response.code

Definition at line 215 of file https.py.

**11.108.3.2 rpki.https.http\_response.reason**

Definition at line 216 of file https.py.

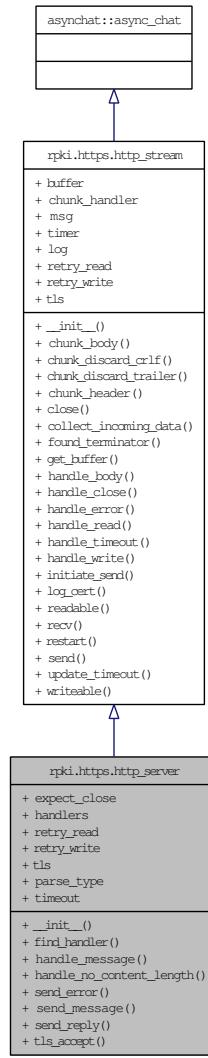
The documentation for this class was generated from the following file:

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

**11.109 rpki.https.http\_server Class Reference**

Inherits [rpki::https::http\\_stream](#).

Collaboration diagram for rpki.https.http\_server:



### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [find\\_handler](#)
- def [handle\\_message](#)
- def [handle\\_no\\_content\\_length](#)
- def [send\\_error](#)

- def [send\\_message](#)
- def [send\\_reply](#)
- def [tls\\_accept](#)

### Public Attributes

- [expect\\_close](#)
- [handlers](#)
- [retry\\_read](#)
- [retry\\_write](#)
- [tls](#)

### Static Public Attributes

- [parse\\_type = http\\_request](#)  
*Stream parser should look for incoming HTTP request messages.*
- [timeout = default\\_server\\_timeout](#)  
*Use the default server timeout value set in the module header.*

### 11.109.1 Detailed Description

HTTP (S) server stream.

Definition at line 561 of file https.py.

### 11.109.2 Member Function Documentation

#### 11.109.2.1 def rpkি.https.http\_server.\_\_init\_\_ ( self, sock, handlers, cert = None, key = None, ta = (), dynamic\_ta = None)

Definition at line 574 of file https.py.

#### 11.109.2.2 def rpkি.https.http\_server.find\_handler ( self, path)

Helper method to search self.handlers.

Definition at line 635 of file https.py.

**11.109.2.3 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.

**11.109.2.4 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.

**11.109.2.5 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.

**11.109.2.6 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.

**11.109.2.7 def rpki.https.http\_server.send\_reply ( *self, code, body* )**

Send a reply to this request.

Definition at line 679 of file https.py.

**11.109.2.8 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.

**11.109.3 Member Data Documentation****11.109.3.1 rpki.https.http\_server.expect\_close**

Definition at line 578 of file https.py.

**11.109.3.2 rpki.https.http\_server.handlers**

Definition at line 576 of file https.py.

**11.109.3.3 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.

**11.109.3.4 rpki.https.http\_server.retry\_read**

Reimplemented from [rpki.https.http\\_stream](#).

Definition at line 613 of file https.py.

**11.109.3.5 rpki.https.http\_server.retry\_write**

Reimplemented from [rpki.https.http\\_stream](#).

Definition at line 615 of file https.py.

**11.109.3.6 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.

**11.109.3.7 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:

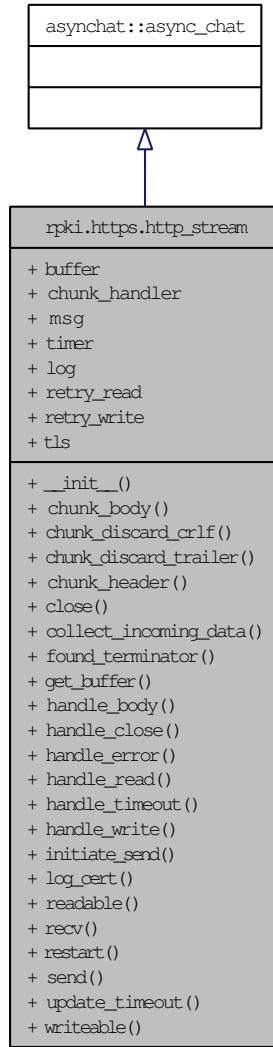
- [https.py \(3191\)](#)

**11.110 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

#### 11.110.1 Detailed Description

Virtual class representing an HTTP message stream.

Definition at line 243 of file https.py.

**11.110.2 Member Function Documentation****11.110.2.1 def rpkি.https.http\_stream.\_\_init\_\_(self, sock = None)**

Definition at line 253 of file https.py.

**11.110.2.2 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.

**11.110.2.3 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.

**11.110.2.4 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.

**11.110.2.5 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.

**11.110.2.6 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.

**11.110.2.7 def rpki.https.http\_stream.collect\_incoming\_data ( *self*, *data*)**

Buffer incoming data from asynchat.

Definition at line 279 of file https.py.

**11.110.2.8 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.

**11.110.2.9 def rpki.https.http\_stream.get\_buffer ( *self*)**

Consume data buffered from asynchat.

Definition at line 286 of file https.py.

**11.110.2.10 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.

**11.110.2.11 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.

**11.110.2.12 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.

**11.110.2.13 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.

**11.110.2.14 def rpki.https.http\_stream.handle\_timeout (*self*)**

Inactivity timer expired, close connection with prejudice.

Reimplemented in [rpki.https.http\\_client](#).

Definition at line 399 of file https.py.

#### **11.110.2.15 def rpki.https.http\_stream.handle\_write (*self*)**

Asyncore says socket is writeable. Make sure there's no TLS read already in progress, retry previous write operation if we had one that was blocked on the socket, otherwise try to write some data. Handling all the weird OpenSSL exceptions that TLS throws is our caller's problem.

Definition at line 478 of file https.py.

#### **11.110.2.16 def rpki.https.http\_stream.initiate\_send (*self*)**

Initiate a write operation. This is just a wrapper around the asynchat method, to handle all the whacky TLS exceptions.

Definition at line 502 of file https.py.

#### **11.110.2.17 def rpki.https.http\_stream.log\_cert (*self, tag, x*)**

Log HTTPS certificates, if certificate debugging is enabled.

Definition at line 554 of file https.py.

#### **11.110.2.18 def rpki.https.http\_stream.readable (*self*)**

TLS replacement for normal asynchat .readable() method. A TLS connection that's blocked waiting for TLS write is considered not readable even if the underlying socket is.

Definition at line 434 of file https.py.

**11.110.2.19 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.

**11.110.2.20 def rpki.https.http\_stream.restart (*self*)**

(Re)start HTTP message parser, reset timer.

Definition at line 259 of file https.py.

**11.110.2.21 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.

**11.110.2.22 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.

**11.110.2.23 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.

**11.110.3 Member Data Documentation****11.110.3.1 rpki.https.http\_stream.buffer**

Definition at line 255 of file https.py.

**11.110.3.2 rpki.https.http\_stream.chunk\_handler**

Definition at line 264 of file https.py.

**11.110.3.3 rpki.https.http\_stream.log = log\_method [static]**

Definition at line 248 of file https.py.

**11.110.3.4 rpki.https.http\_stream.msg**

Definition at line 317 of file https.py.

**11.110.3.5 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.

**11.110.3.6 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.

**11.110.3.7 rpki.https.http\_stream.timer**

Definition at line 256 of file https.py.

#### 11.110.3.8 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.

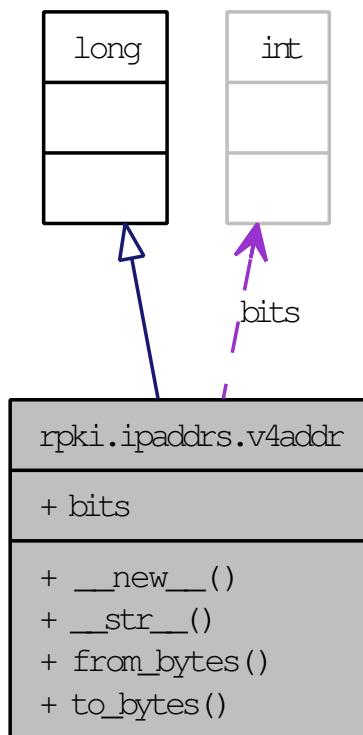
The documentation for this class was generated from the following file:

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

## 11.111 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

#### 11.111.1 Detailed Description

IPv4 address.

Derived from long, but supports IPv4 print syntax.

Definition at line 47 of file ipaddrs.py.

#### 11.111.2 Member Function Documentation

##### 11.111.2.1 def rpk.iipaddrs.v4addr.\_\_new\_\_ (*cls*, *x*)

Construct a v4addr object.

Definition at line 56 of file ipaddrs.py.

##### 11.111.2.2 def rpk.iipaddrs.v4addr.\_\_str\_\_ (*self*)

Convert a v4addr object to string format.

Definition at line 74 of file ipaddrs.py.

##### 11.111.2.3 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.

**11.111.2.4 def rpki.ipaddrs.v4addr.to\_bytes ( *self* )**

Convert a v4addr object to a raw byte string.

Definition at line 65 of file ipaddrs.py.

**11.111.3 Member Data Documentation****11.111.3.1 int rpki.ipaddrs.v4addr.bits = 32 [static]**

Definition at line 54 of file ipaddrs.py.

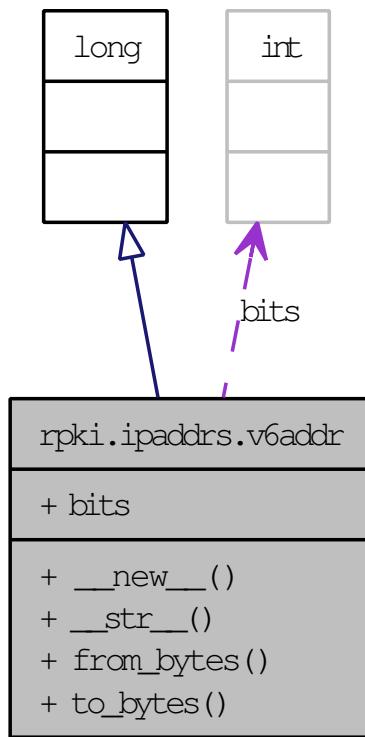
The documentation for this class was generated from the following file:

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

**11.112 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

### 11.112.1 Detailed Description

IPv6 address.

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

Definition at line 78 of file ipaddrs.py.

### 11.112.2 Member Function Documentation

#### 11.112.2.1 def rpk.iipaddrs.v6addr.\_\_new\_\_ (*cls*, *x*)

Construct a v6addr object.

Definition at line 87 of file ipaddrs.py.

#### 11.112.2.2 def rpk.iipaddrs.v6addr.\_\_str\_\_ (*self*)

Convert a v6addr object to string format.

Definition at line 104 of file ipaddrs.py.

#### 11.112.2.3 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.

#### 11.112.2.4 def rpk.iipaddrs.v6addr.to\_bytes (*self*)

Convert a v6addr object to a raw byte string.

Definition at line 94 of file ipaddrs.py.

### 11.112.3 Member Data Documentation

#### 11.112.3.1 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:

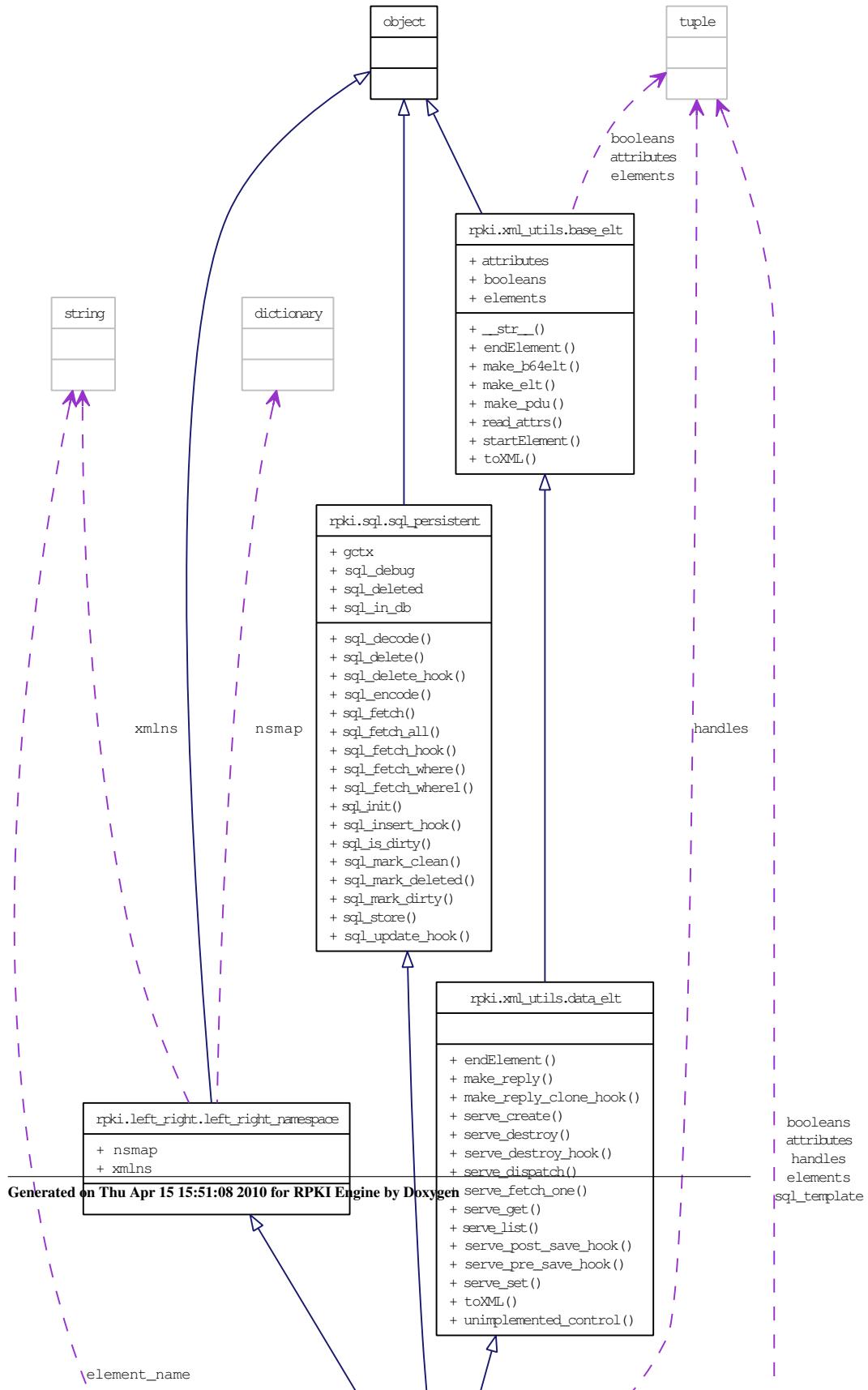
- [ipaddrs.py \(2424\)](#)

## 11.113 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](#)

### 11.113.1 Detailed Description

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

Definition at line 526 of file left\_right.py.

### 11.113.2 Member Function Documentation

#### 11.113.2.1 def rpkি.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.

**11.113.2.2 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.

**11.113.2.3 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.

**11.113.2.4 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.

**11.113.3 Member Data Documentation****11.113.3.1 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.

**11.113.3.2 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.

#### **11.113.3.3 string rpkি.left\_right.bsc\_elt.element\_name = "bsc" [static]**

Definition at line 531 of file left\_right.py.

#### **11.113.3.4 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.

#### **11.113.3.5 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.

#### **11.113.3.6 rpkি.left\_right.bsc\_elt.pkcs10\_request = None [static]**

Definition at line 545 of file left\_right.py.

#### **11.113.3.7 rpkি.left\_right.bsc\_elt.private\_key\_id = None [static]**

Definition at line 544 of file left\_right.py.

#### **11.113.3.8 rpkি.left\_right.bsc\_elt.signing\_cert = None [static]**

Reimplemented in [irbe\\_cli.bsc\\_elt](#).

Definition at line 546 of file left\_right.py.

### 11.113.3.9 rpki.left\_right.bsc\_elt.signing\_cert\_crl = None [static]

Reimplemented in [irbe\\_cli.bsc\\_elt](#).

Definition at line 547 of file left\_right.py.

### 11.113.3.10 tuple rpki.left\_right.bsc\_elt.sql\_template [static]

**Initial value:**

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

Definition at line 536 of file left\_right.py.

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

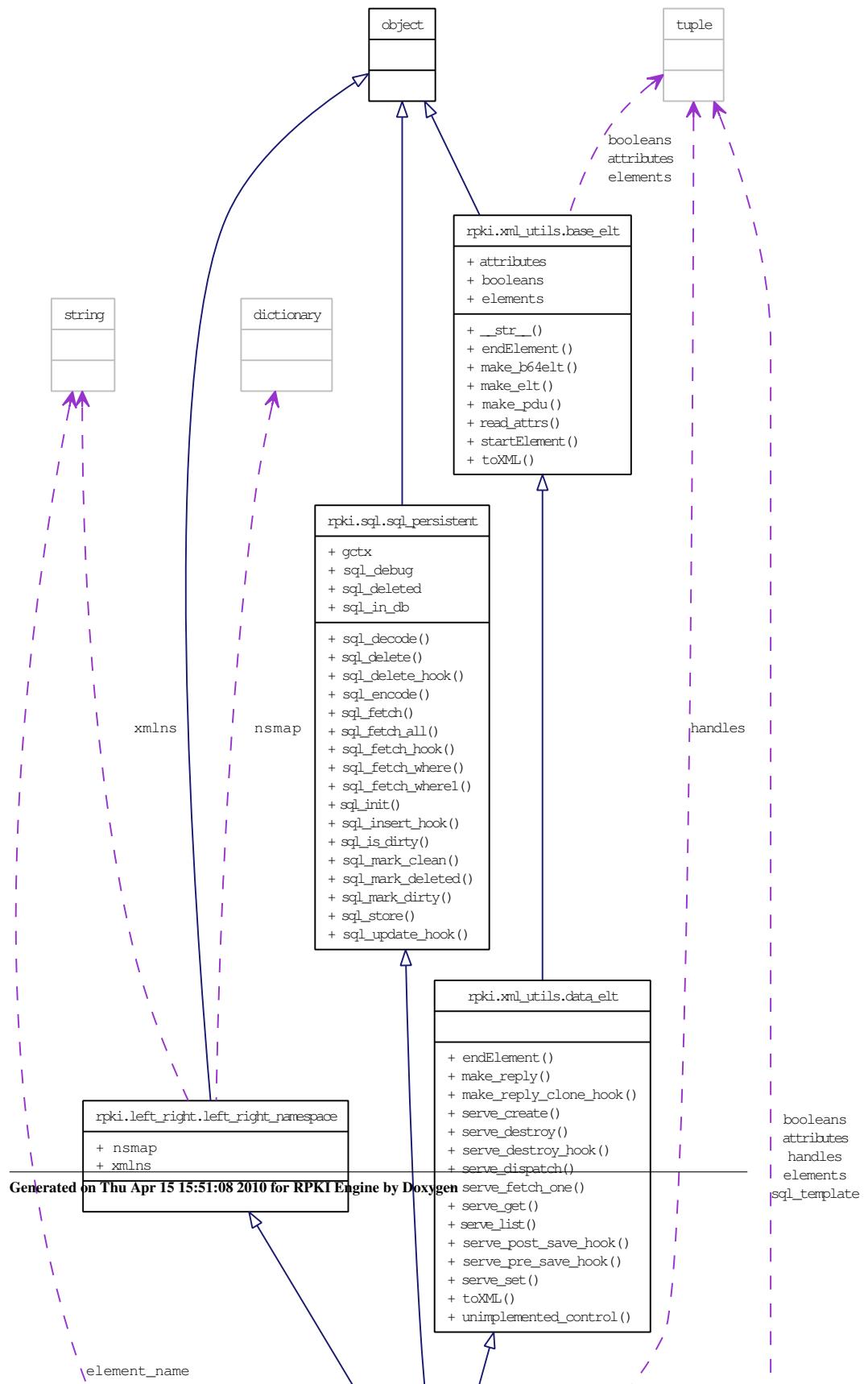
- [left\\_right.py \(3191\)](#)

## 11.114 rpki.left\_right.child\_elt Class Reference

Inherits [rpki::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` = ("bpki\_cert", "bpki\_glue")

*XML elements contained by this element.*

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

- tuple `sql_template`

#### 11.114.1 Detailed Description

`<child/>` element.

Definition at line 805 of file left\_right.py.

#### 11.114.2 Member Function Documentation

##### 11.114.2.1 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.

**11.114.2.2 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.

**11.114.2.3 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.

**11.114.2.4 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.

**11.114.2.5 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.

**11.114.2.6 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.

**11.114.2.7 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.

**11.114.3 Member Data Documentation****11.114.3.1 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.

**11.114.3.2 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.

**11.114.3.3 rpki.left\_right.child\_elt.bpkki\_cert = None [static]**

Definition at line 822 of file left\_right.py.

**11.114.3.4 rpki.left\_right.child\_elt.bpkki\_glue = None [static]**

Definition at line 823 of file left\_right.py.

**11.114.3.5 rpki.left\_right.child\_elt.clear\_https\_ta\_cache = False [static]**

Definition at line 824 of file left\_right.py.

**11.114.3.6 string rpki.left\_right.child\_elt.element\_name = "child" [static]**

Definition at line 810 of file left\_right.py.

**11.114.3.7 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.

**11.114.3.8 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.

**11.114.3.9 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:

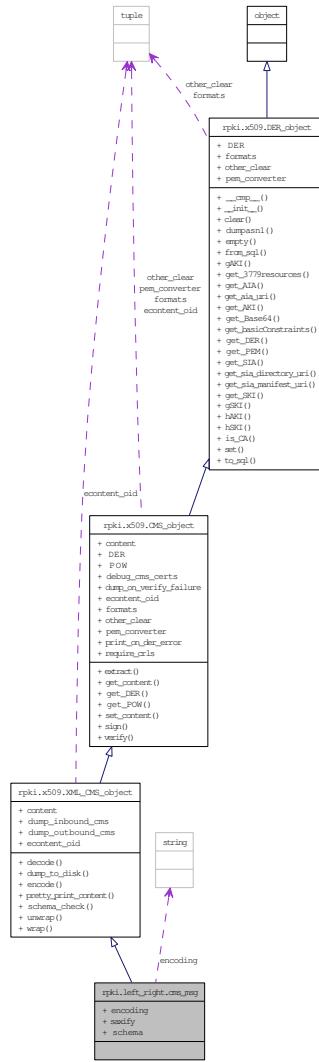
- [left\\_right.py \(3191\)](#)

**11.115 rpki.left\_right.cms\_msg Class Reference**

Inherits [rpki::x509::XML\\_CMS\\_object](#).

Inherited by [irbe\\_cli.left\\_right\\_cms\\_msg](#).

Collaboration diagram for rpkic.left\_right.cms\_msg:



### Static Public Attributes

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

### 11.115.1 Detailed Description

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

Definition at line 1120 of file left\_right.py.

### 11.115.2 Member Data Documentation

#### 11.115.2.1 string rpki.left\_right.cms\_msg.encoding = "us-ascii" [static]

Definition at line 1125 of file left\_right.py.

#### 11.115.2.2 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.

#### 11.115.2.3 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:

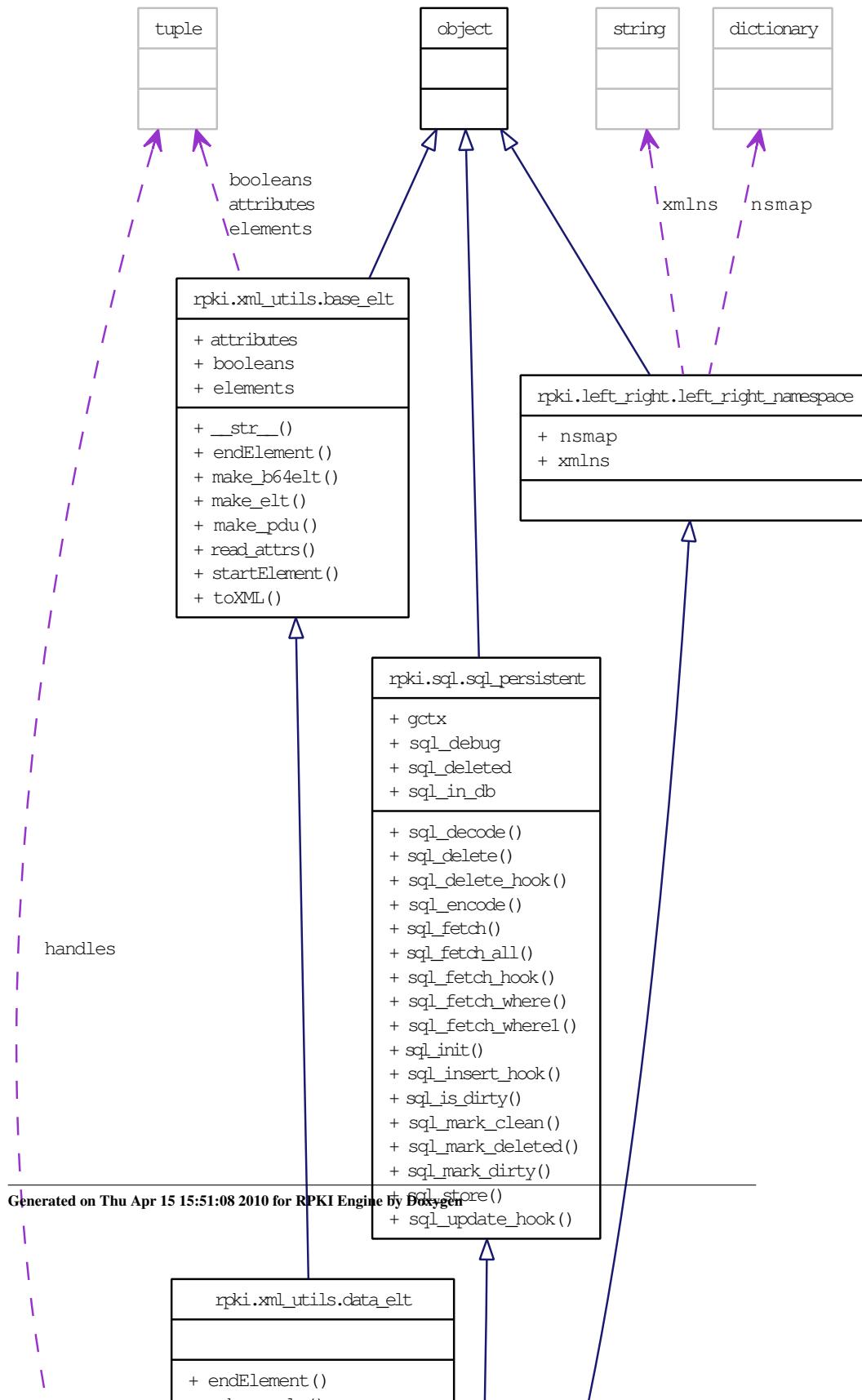
- [left\\_right.py \(3191\)](#)

## 11.116 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

### 11.116.1 Detailed Description

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

Definition at line 50 of file left\_right.py.

### 11.116.2 Member Function Documentation

#### 11.116.2.1 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.

#### 11.116.2.2 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.

**11.116.2.3 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.

**11.116.2.4 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.

**11.116.2.5 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.

**11.116.2.6 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.

**11.116.2.7 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.

### 11.116.3 Member Data Documentation

#### 11.116.3.1 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.

#### 11.116.3.2 rpki.left\_right.data\_elt.self\_handle = None [static]

Definition at line 58 of file left\_right.py.

#### 11.116.3.3 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:

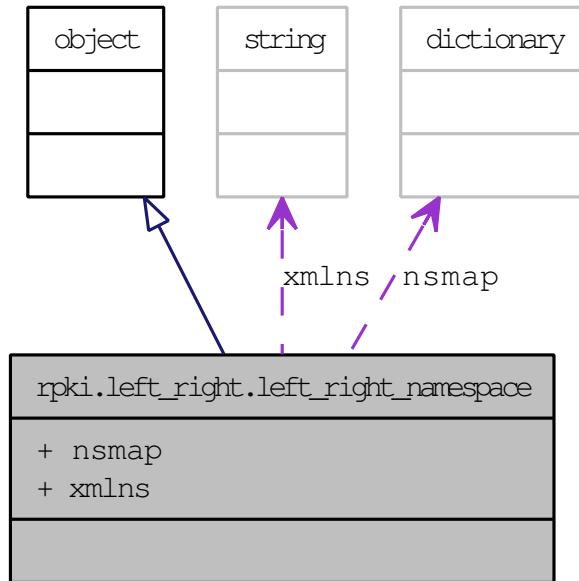
- [left\\_right.py \(3191\)](#)

## 11.117 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/"

### 11.117.1 Detailed Description

XML namespace parameters for left-right protocol.

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

### 11.117.2 Member Data Documentation

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

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

```
11.117.2.2 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:

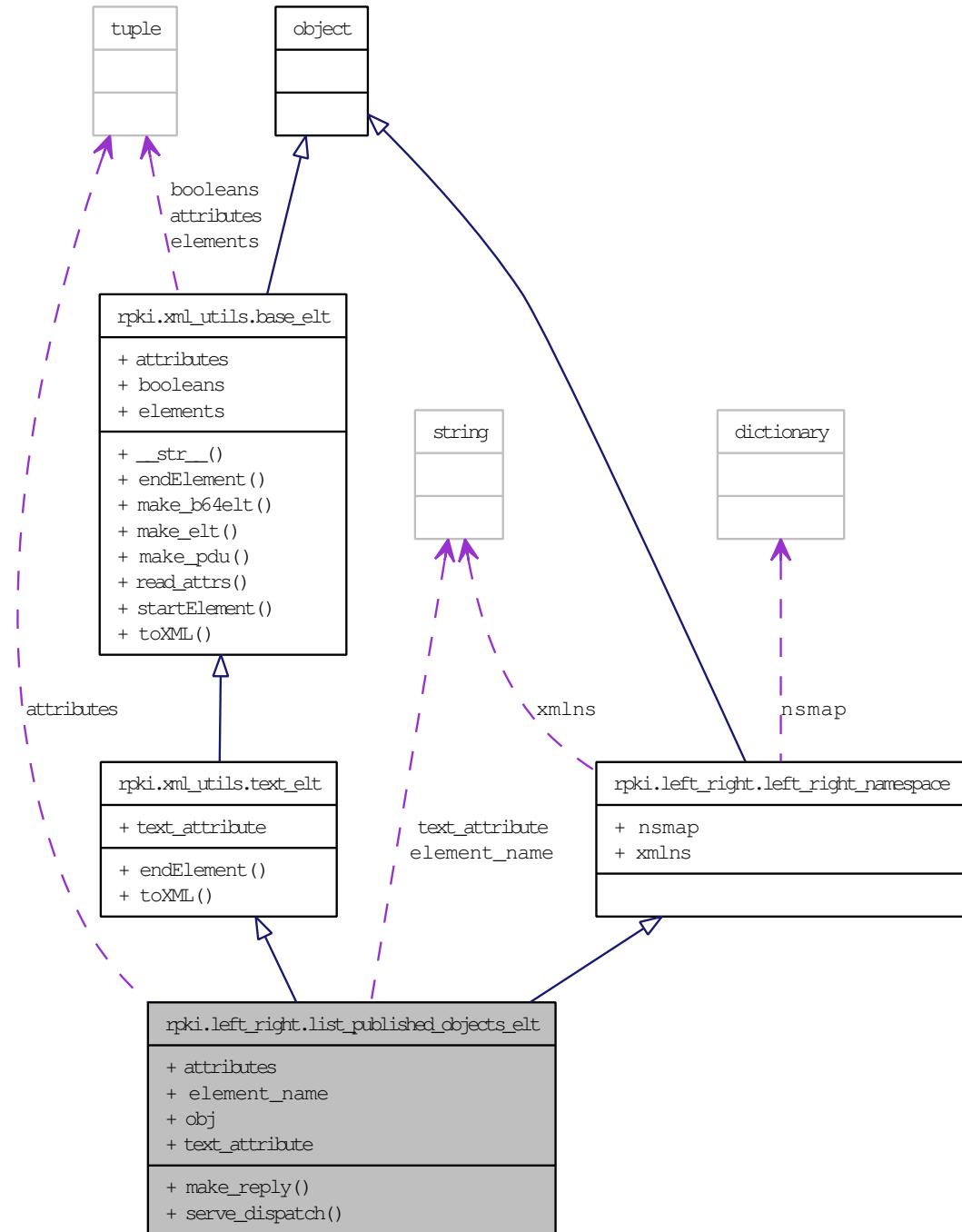
- [left\\_right.py \(3191\)](#)

## 11.118 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.*

#### 11.118.1 Detailed Description

<list\_published\_objects/> element.

Definition at line 968 of file left\_right.py.

#### 11.118.2 Member Function Documentation

##### 11.118.2.1 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.

##### 11.118.2.2 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.

### 11.118.3 Member Data Documentation

**11.118.3.1 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.

**11.118.3.2 string `rpk.left_right.list_published_objects_elt.element_name` = "list\_published\_objects" [static]**

Definition at line 973 of file left\_right.py.

**11.118.3.3 `rpk.left_right.list_published_objects_elt.obj` = None [static]**

Definition at line 977 of file left\_right.py.

**11.118.3.4 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:

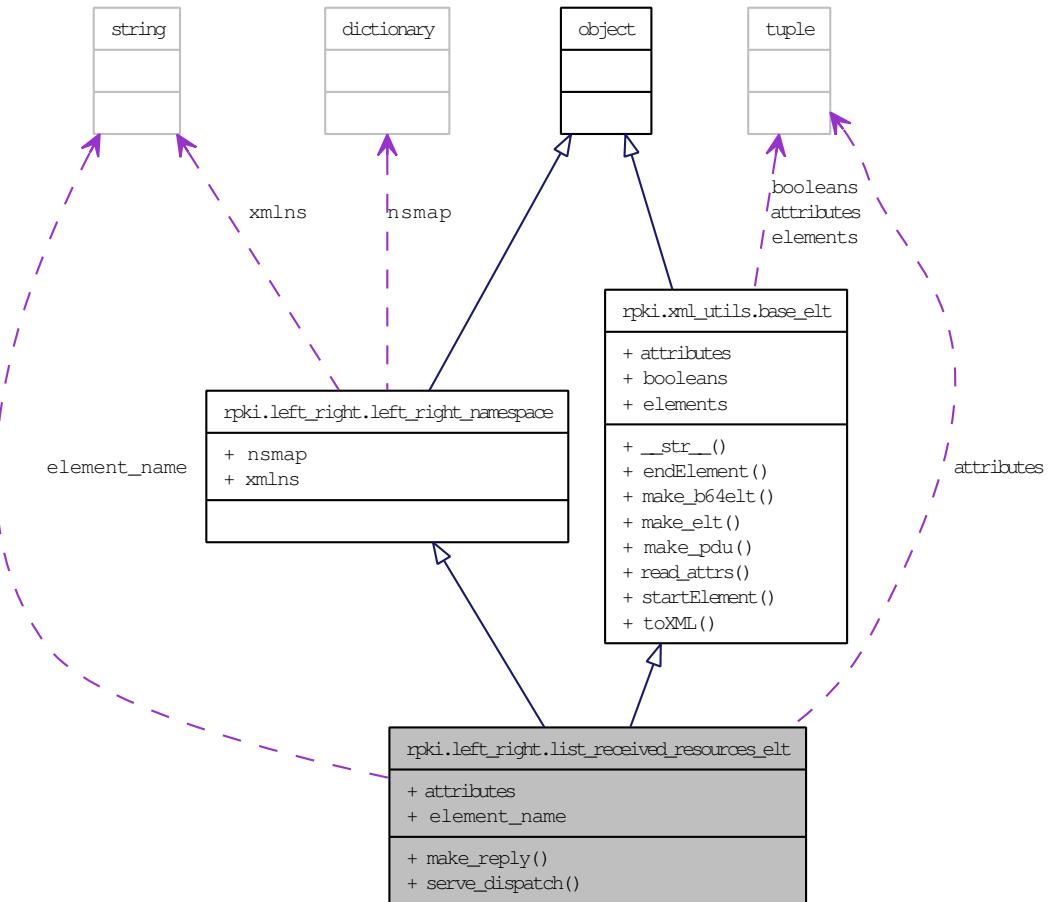
- [left\\_right.py \(3191\)](#)

## 11.119 `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"

### 11.119.1 Detailed Description

<list\_received\_resources/> element.

Definition at line 1003 of file left\_right.py.

### 11.119.2 Member Function Documentation

#### 11.119.2.1 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.

#### 11.119.2.2 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.

### 11.119.3 Member Data Documentation

#### 11.119.3.1 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.

**11.119.3.2 string rpki.left\_right.list\_received\_resources\_elt.element\_name =  
"list\_received\_resources" [static]**

Definition at line 1008 of file left\_right.py.

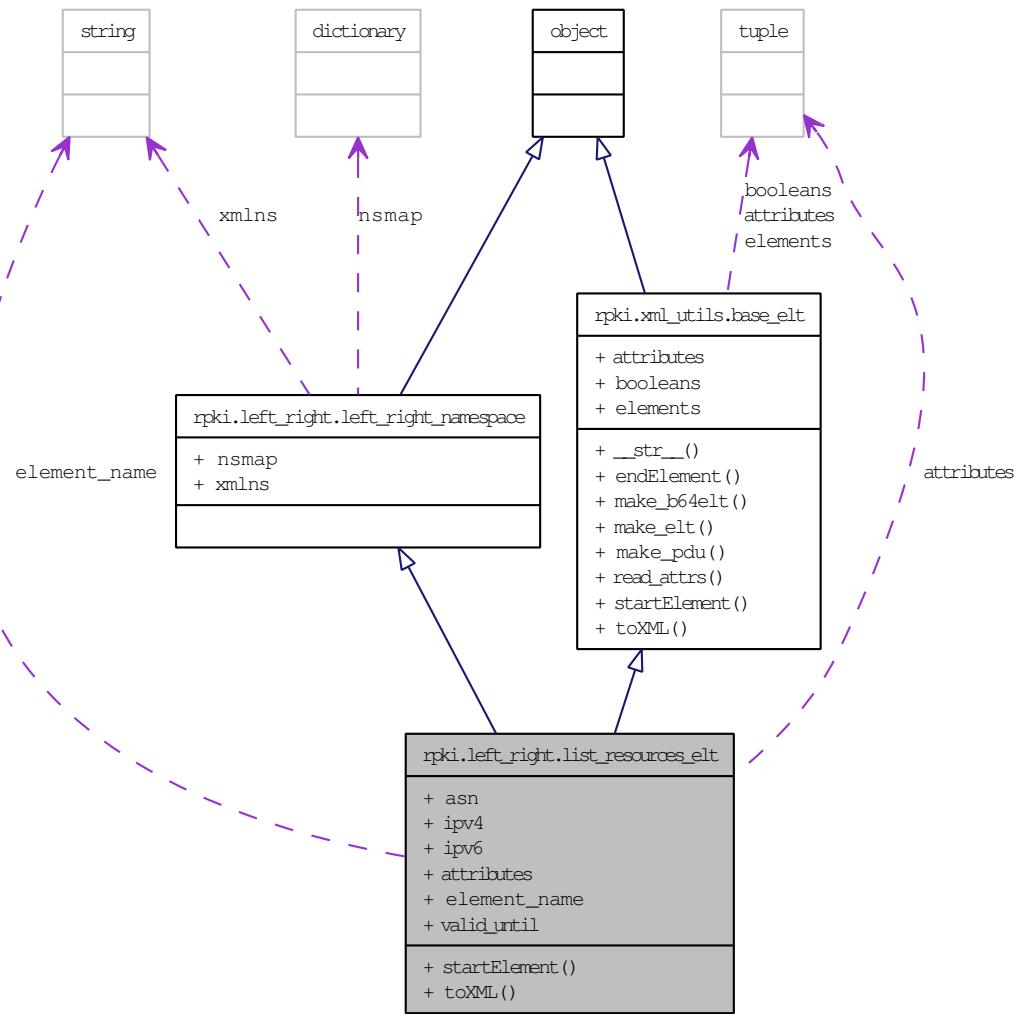
The documentation for this class was generated from the following file:

- [left\\_right.py \(3191\)](#)

## 11.120 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

### 11.120.1 Detailed Description

<list\_resources/> element.

Definition at line 913 of file left\_right.py.

### 11.120.2 Member Function Documentation

#### 11.120.2.1 def rpk.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 [rpk.xml\\_utils.base\\_elt](#).

Definition at line 922 of file left\_right.py.

#### 11.120.2.2 def rpk.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 [rpk.xml\\_utils.base\\_elt](#).

Definition at line 938 of file left\_right.py.

**11.120.3 Member Data Documentation****11.120.3.1 rpki.left\_right.list\_resources\_elt.asn**

Definition at line 932 of file left\_right.py.

```
11.120.3.2 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.

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

Definition at line 918 of file left\_right.py.

**11.120.3.4 rpki.left\_right.list\_resources\_elt.ipv4**

Definition at line 934 of file left\_right.py.

**11.120.3.5 rpki.left\_right.list\_resources\_elt.ipv6**

Definition at line 936 of file left\_right.py.

```
11.120.3.6 rpki.left_right.list_resources_elt.valid_until = None [static]
```

Definition at line 920 of file left\_right.py.

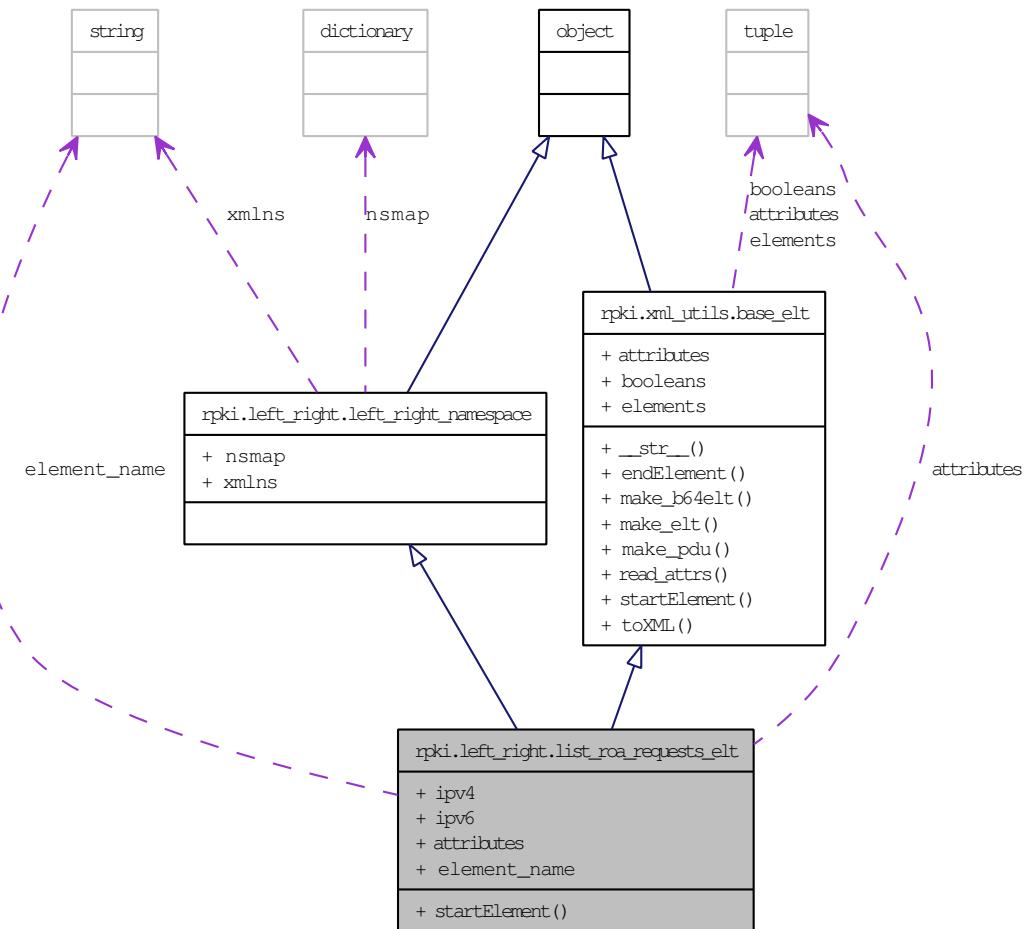
The documentation for this class was generated from the following file:

- [left\\_right.py \(3191\)](#)

## 11.121 rpk.left\_right.list\_roa\_requests\_elt Class Reference

Inherits [rpk::xml\\_utils::base\\_elt](#), and [rpk::left\\_right::left\\_right\\_namespace](#).

Collaboration diagram for rpk.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"

### 11.121.1 Detailed Description

<list\_roa\_requests/> element.

Definition at line 948 of file left\_right.py.

### 11.121.2 Member Function Documentation

#### 11.121.2.1 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.

### 11.121.3 Member Data Documentation

#### 11.121.3.1 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.

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

Definition at line 953 of file left\_right.py.

```
11.121.3.3 rpki.left_right.list_roa_requests_elt.ipv4
```

Definition at line 964 of file left\_right.py.

```
11.121.3.4 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:

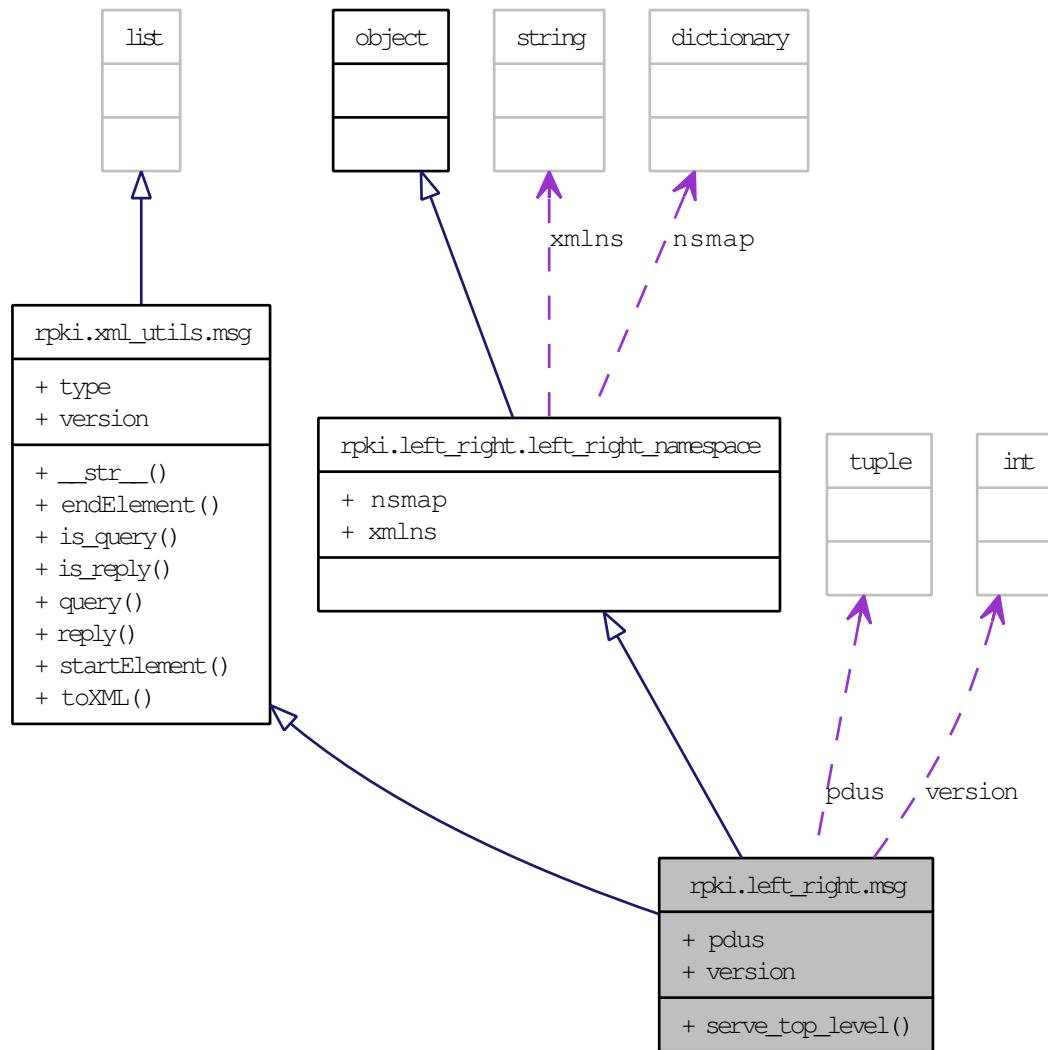
- [left\\_right.py \(3191\)](#)

## 11.122 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.*

### 11.122.1 Detailed Description

Left-right PDU.

Definition at line 1066 of file left\_right.py.

### 11.122.2 Member Function Documentation

#### 11.122.2.1 def rpki.left\_right.msg.serve\_top\_level (*self, gctx, cb*)

Serve one msg PDU.

Definition at line 1083 of file left\_right.py.

### 11.122.3 Member Data Documentation

#### 11.122.3.1 rpki::left\_right.msg::pdus [static]

**Initial value:**

```
dict((x.element_name, x)
     for x in (self_elt, child_elt, parent_elt, bsc_elt, repository_elt,
               list_resources_elt, list_roa_requests_elt,
               list_published_objects_elt, list_received_resources_elt,
               report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented in [irbe\\_cli.left\\_right\\_msg](#).

Definition at line 1077 of file left\_right.py.

#### 11.122.3.2 rpki::left\_right.msg::version = 1 [static]

Protocol version.

Reimplemented from [rpk.xml\\_utils.msg](#).

Definition at line 1073 of file [left\\_right.py](#).

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

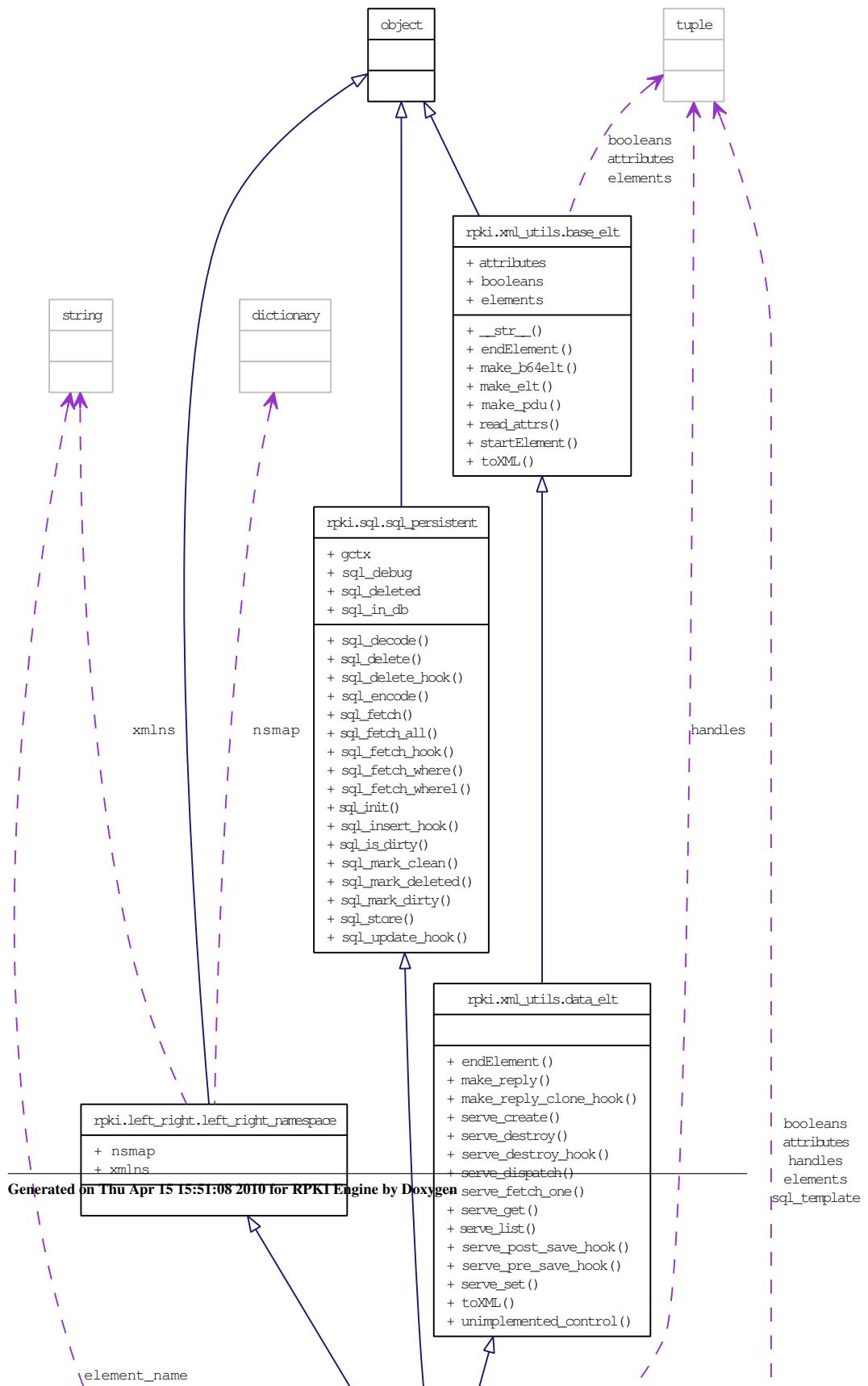
- [left\\_right.py \(3191\)](#)

## 11.123 rpk.left\_right.parent\_elt Class Reference

Inherits [rpk::left\\_right::data\\_elt](#).

Inherited by [irbe\\_cli.parent\\_elt](#).

## Collaboration diagram for rpki.left\_right.parent\_elt:



### Public Member Functions

- def `cas`
- def `query_up_down`
- def `repository`
- def `serve_post_save_hook`
- def `serve_rekey`
- def `serve_revoke`
- def `serve_revoke_forgotten`

### Static Public Attributes

- tuple `attributes`  
*XML attributes for this element.*
- tuple `booleans` = ("rekey", "reissue", "revoke", "revoke\_forgotten")  
*Boolean attributes (value "yes" or "no") for this element.*
- `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`

#### 11.123.1 Detailed Description

<parent/> element.

Definition at line 656 of file left\_right.py.

#### 11.123.2 Member Function Documentation

##### 11.123.2.1 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.

**11.123.2.2 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.

**11.123.2.3 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.

**11.123.2.4 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.

**11.123.2.5 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.

**11.123.2.6 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.

**11.123.2.7 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.

**11.123.3 Member Data Documentation****11.123.3.1 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.

**11.123.3.2 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.

**11.123.3.3 rpk.left\_right.parent\_elt.bpk\_cms\_cert = None [static]**

Definition at line 674 of file left\_right.py.

**11.123.3.4 rpki.left\_right.parent\_elt.bpkı\_cms\_glue = None [static]**

Definition at line 675 of file left\_right.py.

**11.123.3.5 rpki.left\_right.parent\_elt.bpkı\_https\_cert = None [static]**

Definition at line 676 of file left\_right.py.

**11.123.3.6 rpki.left\_right.parent\_elt.bpkı\_https\_glue = None [static]**

Definition at line 677 of file left\_right.py.

**11.123.3.7 string rpki.left\_right.parent\_elt.element\_name = "parent" [static]**

Definition at line 661 of file left\_right.py.

**11.123.3.8 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.

**11.123.3.9 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.

**11.123.3.10 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:

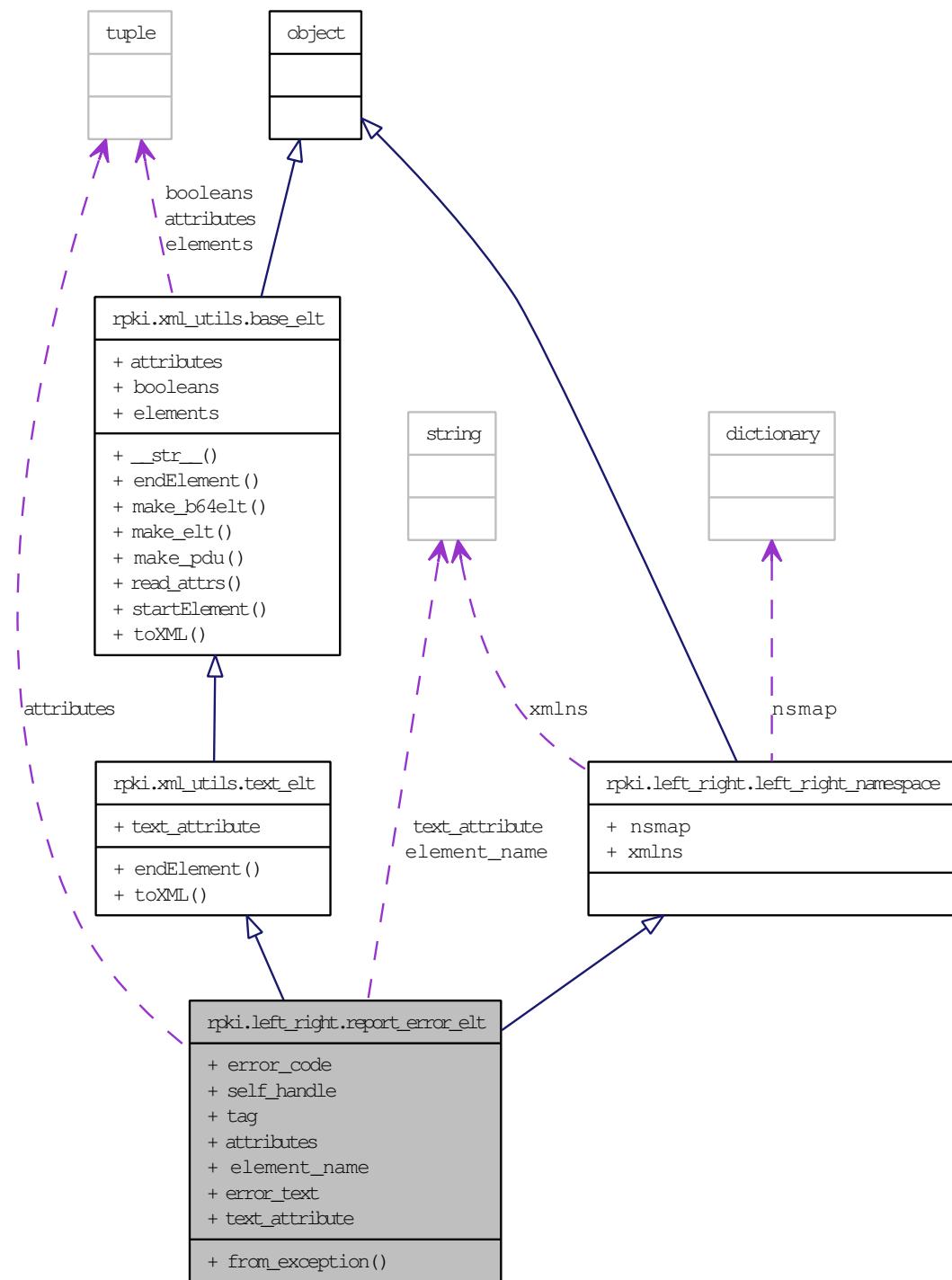
- [left\\_right.py \(3191\)](#)

**11.124 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 rpki.left\_right.report\_error\_elt:



### Public Member Functions

- def [from\\_exception](#)

### Public Attributes

- [error\\_code](#)
- [self\\_handle](#)
- [tag](#)

### Static Public Attributes

- tuple [attributes](#) = ("tag", "self\_handle", "error\_code")

*XML attributes for this element.*

- string [element\\_name](#) = "report\_error"
- [error\\_text](#) = None
- string [text\\_attribute](#) = "error\_text"

*Name of the class attribute that holds the text value.*

### 11.124.1 Detailed Description

<report\_error/> element.

Definition at line 1043 of file left\_right.py.

### 11.124.2 Member Function Documentation

#### 11.124.2.1 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.

### 11.124.3 Member Data Documentation

**11.124.3.1 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.

**11.124.3.2 string rpk.left\_right.report\_error\_elt.element\_name = "report\_error" [static]**

Definition at line 1048 of file left\_right.py.

**11.124.3.3 rpk.left\_right.report\_error\_elt.error\_code**

Definition at line 1062 of file left\_right.py.

**11.124.3.4 rpk.left\_right.report\_error\_elt.error\_text = None [static]**

Definition at line 1052 of file left\_right.py.

**11.124.3.5 rpk.left\_right.report\_error\_elt.self\_handle**

Definition at line 1060 of file left\_right.py.

**11.124.3.6 rpk.left\_right.report\_error\_elt.tag**

Definition at line 1061 of file left\_right.py.

**11.124.3.7 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:

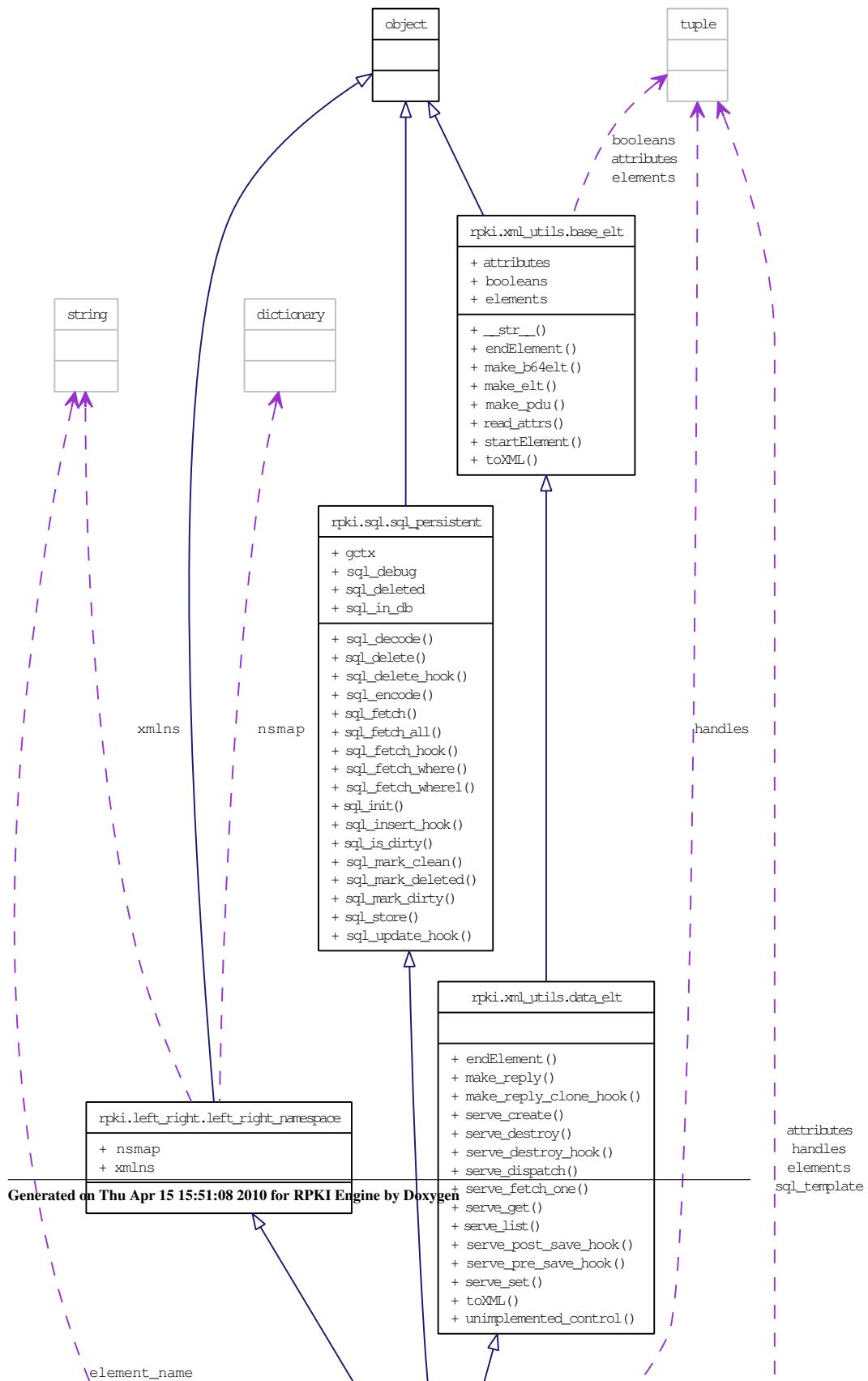
- [left\\_right.py \(3191\)](#)

**11.125 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`

### 11.125.1 Detailed Description

`<repository/>` element.

Definition at line 573 of file `left_right.py`.

### 11.125.2 Member Function Documentation

#### 11.125.2.1 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`.

**11.125.2.2 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.

**11.125.2.3 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.

**11.125.3 Member Data Documentation****11.125.3.1 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.

**11.125.3.2 rpk.left\_right.repository\_elt.bpk.cert = None [static]**

Definition at line 587 of file left\_right.py.

**11.125.3.3 rpk.left\_right.repository\_elt.bpk.glue = None [static]**

Definition at line 588 of file left\_right.py.

**11.125.3.4 string rpk.left\_right.repository\_elt.element\_name = "repository" [static]**

Definition at line 578 of file left\_right.py.

**11.125.3.5 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.

**11.125.3.6 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.

**11.125.3.7 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:

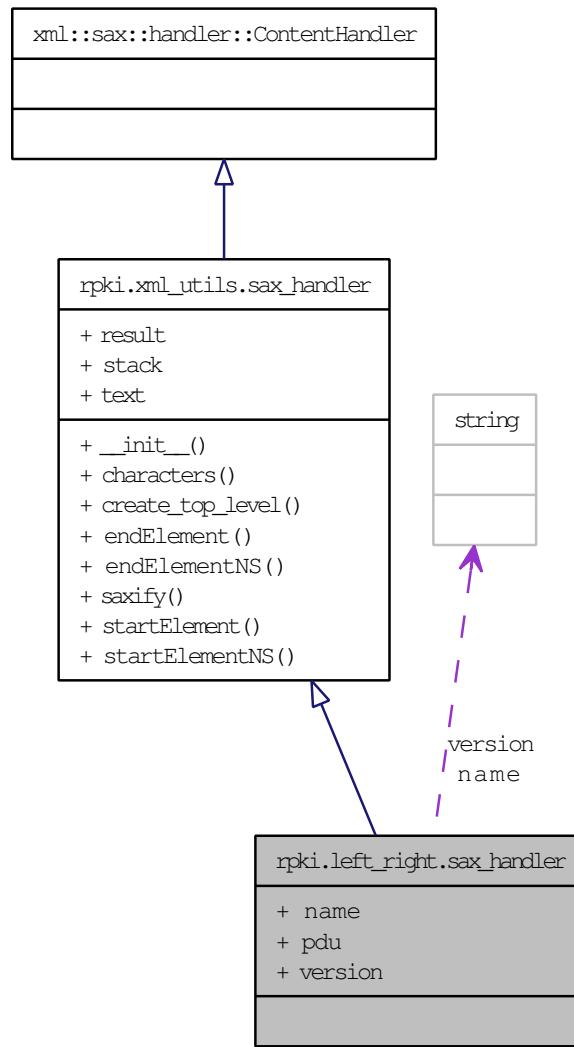
- [left\\_right.py \(3191\)](#)

## 11.126 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"

### 11.126.1 Detailed Description

SAX handler for Left-Right protocol.

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

### 11.126.2 Member Data Documentation

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

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

#### 11.126.2.2 `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`.

#### 11.126.2.3 `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:

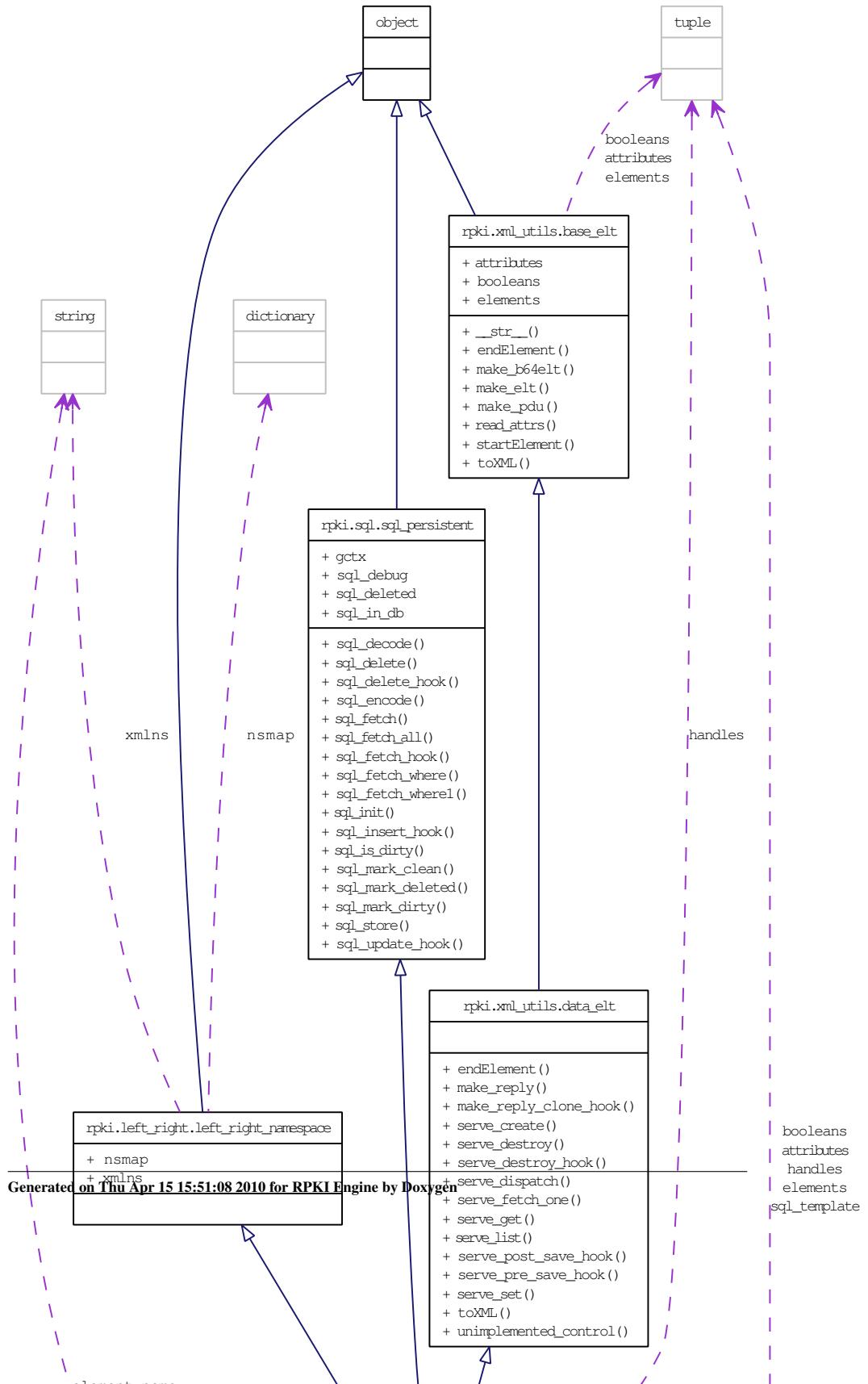
- [left\\_right.py \(3191\)](#)

## 11.127 `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

### 11.127.1 Detailed Description

<self/> element.

Definition at line 124 of file left\_right.py.

### 11.127.2 Member Function Documentation

#### 11.127.2.1 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.

#### 11.127.2.2 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.

#### 11.127.2.3 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.

#### 11.127.2.4 def rpk.left\_right.self\_elt.cron (*self, cb*)

Periodic tasks.

Definition at line 274 of file left\_right.py.

**11.127.2.5 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.

**11.127.2.6 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.

**11.127.2.7 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.

**11.127.2.8 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.

**11.127.2.9 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.

#### 11.127.2.10 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.

#### 11.127.2.11 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.

#### 11.127.2.12 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.

#### 11.127.2.13 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.

#### 11.127.2.14 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.

#### 11.127.2.15 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.

#### 11.127.2.16 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.

#### 11.127.2.17 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.

**11.127.2.18 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.

**11.127.2.19 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.

**11.127.3 Member Data Documentation****11.127.3.1 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.

**11.127.3.2 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.

**11.127.3.3 rpkি.left\_right.self\_elt.bpkি\_cert = None [static]**

Definition at line 142 of file left\_right.py.

**11.127.3.4 rpki.left\_right.self\_elt.bpkiglue = None [static]**

Definition at line 143 of file left\_right.py.

**11.127.3.5 rpki.left\_right.self\_elt.crl\_interval = None [static]**

Definition at line 140 of file left\_right.py.

**11.127.3.6 string rpki.left\_right.self\_elt.element\_name = "self" [static]**

Definition at line 129 of file left\_right.py.

**11.127.3.7 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.

**11.127.3.8 tuple rpki.left\_right.self\_elt.handles = () [static]**

Reimplemented from [rpki.left\\_right.data\\_elt](#).

Definition at line 137 of file left\_right.py.

**11.127.3.9 rpki.left\_right.self\_elt.regen\_margin = None [static]**

Definition at line 141 of file left\_right.py.

**11.127.3.10 tuple rpki.left\_right.self\_elt.sql\_template [static]**

**Initial value:**

```
rpkilog.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.

### 11.127.3.11 rpkilog.left\_right.self\_elt.use\_hsm = False [static]

Definition at line 139 of file left\_right.py.

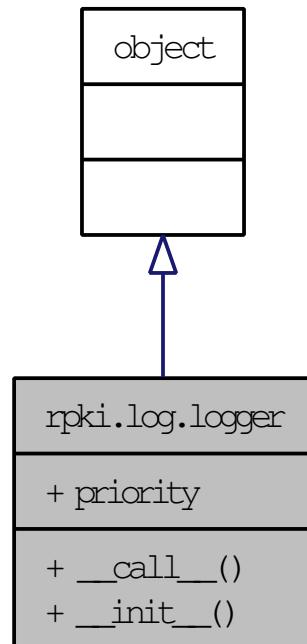
The documentation for this class was generated from the following file:

- [left\\_right.py \(3191\)](#)

## 11.128 rpkilog.logger Class Reference

Inherits [object](#).

Collaboration diagram for rpkilog.logger:



### Public Member Functions

- def [\\_\\_call\\_\\_](#)
- def [\\_\\_init\\_\\_](#)

### Public Attributes

- [priority](#)

#### 11.128.1 Detailed Description

Closure for logging.

Definition at line 71 of file log.py.

#### 11.128.2 Member Function Documentation

##### 11.128.2.1 def rpkilogger.\_\_call\_\_ (*self*, *message*)

Definition at line 79 of file log.py.

##### 11.128.2.2 def rpkilogger.\_\_init\_\_ (*self*, *priority*)

Definition at line 76 of file log.py.

#### 11.128.3 Member Data Documentation

##### 11.128.3.1 rpkilogger.priority

Definition at line 77 of file log.py.

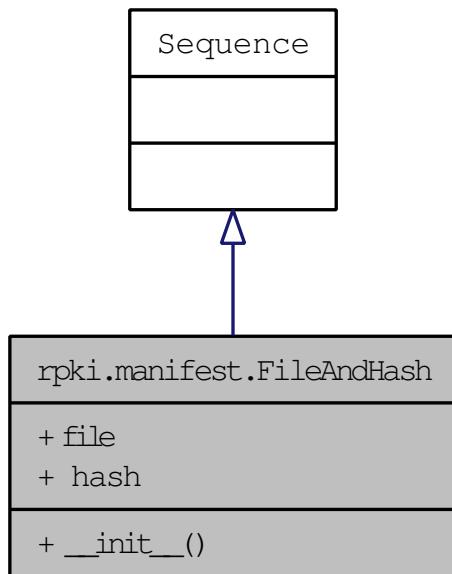
The documentation for this class was generated from the following file:

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

## 11.129 rpkimaniifest.FileAndHash Class Reference

Inherits [Sequence](#).

Collaboration diagram for rpkimaniifest.FileAndHash:



### Public Member Functions

- def [\\_\\_init\\_\\_](#)

### Public Attributes

- [file](#)
- [hash](#)

### 11.129.1 Detailed Description

Definition at line 27 of file manifest.py.

### 11.129.2 Member Function Documentation

**11.129.2.1 def rpkি.manifest.FileAndHash.\_\_init\_\_ ( *self*, *optional* = 0, *default* = ”)**

Definition at line 28 of file manifest.py.

### 11.129.3 Member Data Documentation

**11.129.3.1 rpkি.manifest.FileAndHash.file**

Definition at line 29 of file manifest.py.

**11.129.3.2 rpkি.manifest.FileAndHash.hash**

Definition at line 30 of file manifest.py.

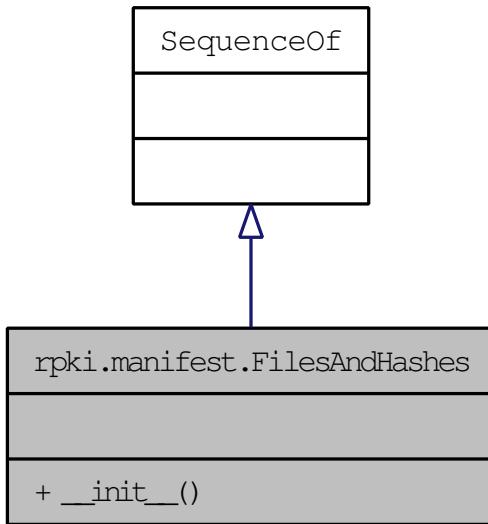
The documentation for this class was generated from the following file:

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

## 11.130 rpkি.manifest.FilesAndHashes Class Reference

Inherits [SequenceOf](#).

Collaboration diagram for rpkি.manifest.FilesAndHashes:



## Public Member Functions

- def `__init__`

### 11.130.1 Detailed Description

Definition at line 34 of file manifest.py.

### 11.130.2 Member Function Documentation

#### 11.130.2.1 def rpkি.manifest.FilesAndHashes.\_\_init\_\_ (*self*, *optional* = 0, *default* = "")

Definition at line 35 of file manifest.py.

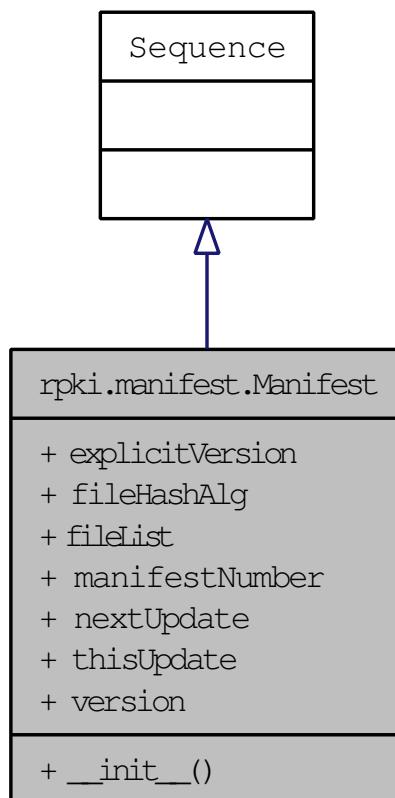
The documentation for this class was generated from the following file:

- `manifest.py (2424)`

## 11.131 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](#)

### 11.131.1 Detailed Description

Definition at line 38 of file manifest.py.

### 11.131.2 Member Function Documentation

#### 11.131.2.1 def rpkি.manifest.Manifest.\_\_init\_\_ (*self*, *optional* = 0, *default* = "")

Definition at line 39 of file manifest.py.

### 11.131.3 Member Data Documentation

#### 11.131.3.1 rpkি.manifest.Manifest.explicitVersion

Definition at line 41 of file manifest.py.

#### 11.131.3.2 rpkি.manifest.Manifest.fileHashAlg

Definition at line 45 of file manifest.py.

#### 11.131.3.3 rpkি.manifest.Manifest fileList

Definition at line 46 of file manifest.py.

#### 11.131.3.4 rpkি.manifest.Manifest.manifestNumber

Definition at line 42 of file manifest.py.

**11.131.3.5 rpki.manifest.Manifest.nextUpdate**

Definition at line 44 of file manifest.py.

**11.131.3.6 rpki.manifest.Manifest.thisUpdate**

Definition at line 43 of file manifest.py.

**11.131.3.7 rpki.manifest.Manifest.version**

Definition at line 40 of file manifest.py.

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

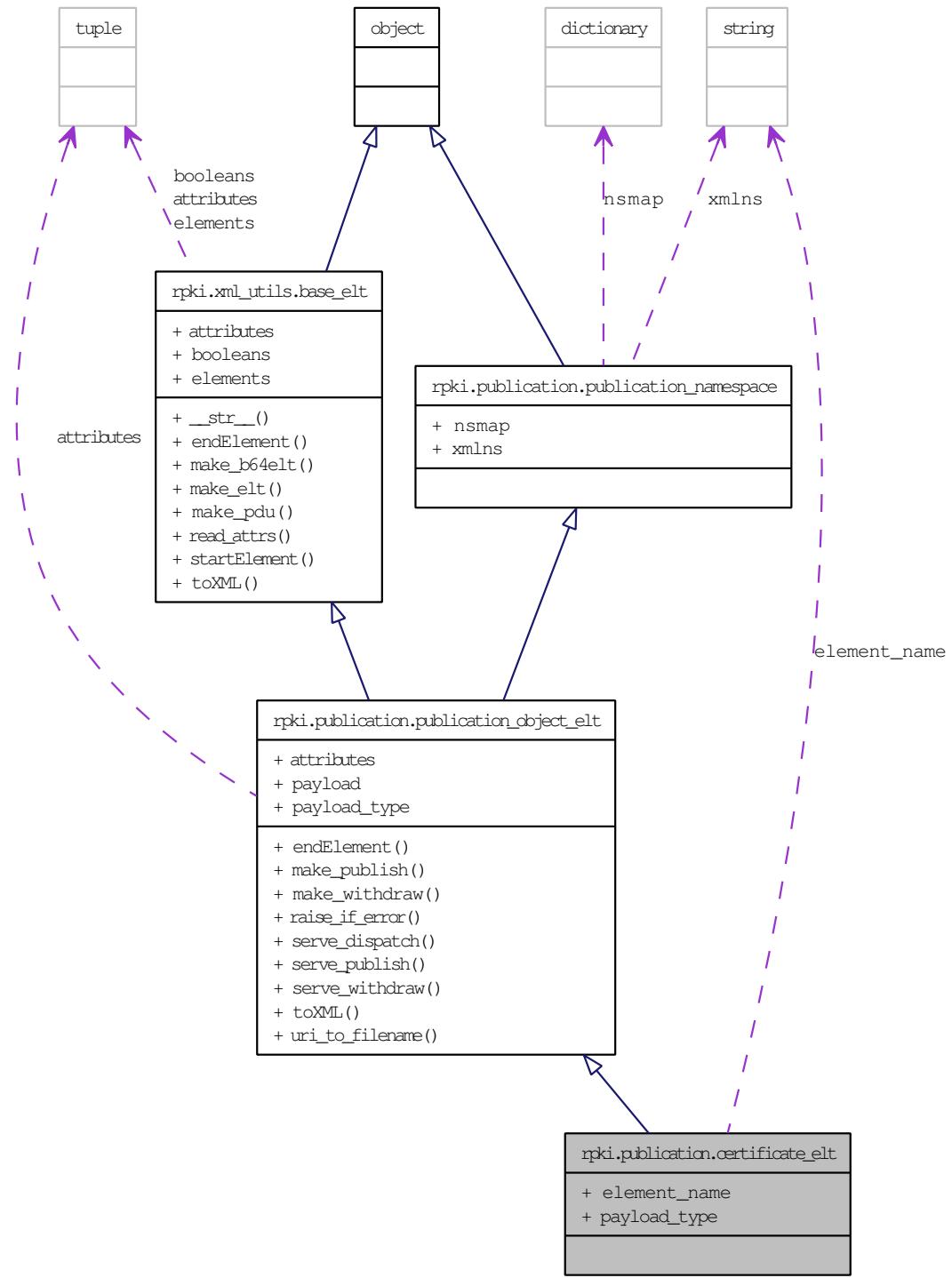
- [manifest.py \(2424\)](#)

**11.132 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`

**11.132.1 Detailed Description**

<certificate/> element.

Definition at line 287 of file publication.py.

**11.132.2 Member Data Documentation****11.132.2.1 string rpk.publication.certificate\_elt.element\_name = "certificate"  
[static]**

Definition at line 292 of file publication.py.

**11.132.2.2 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:

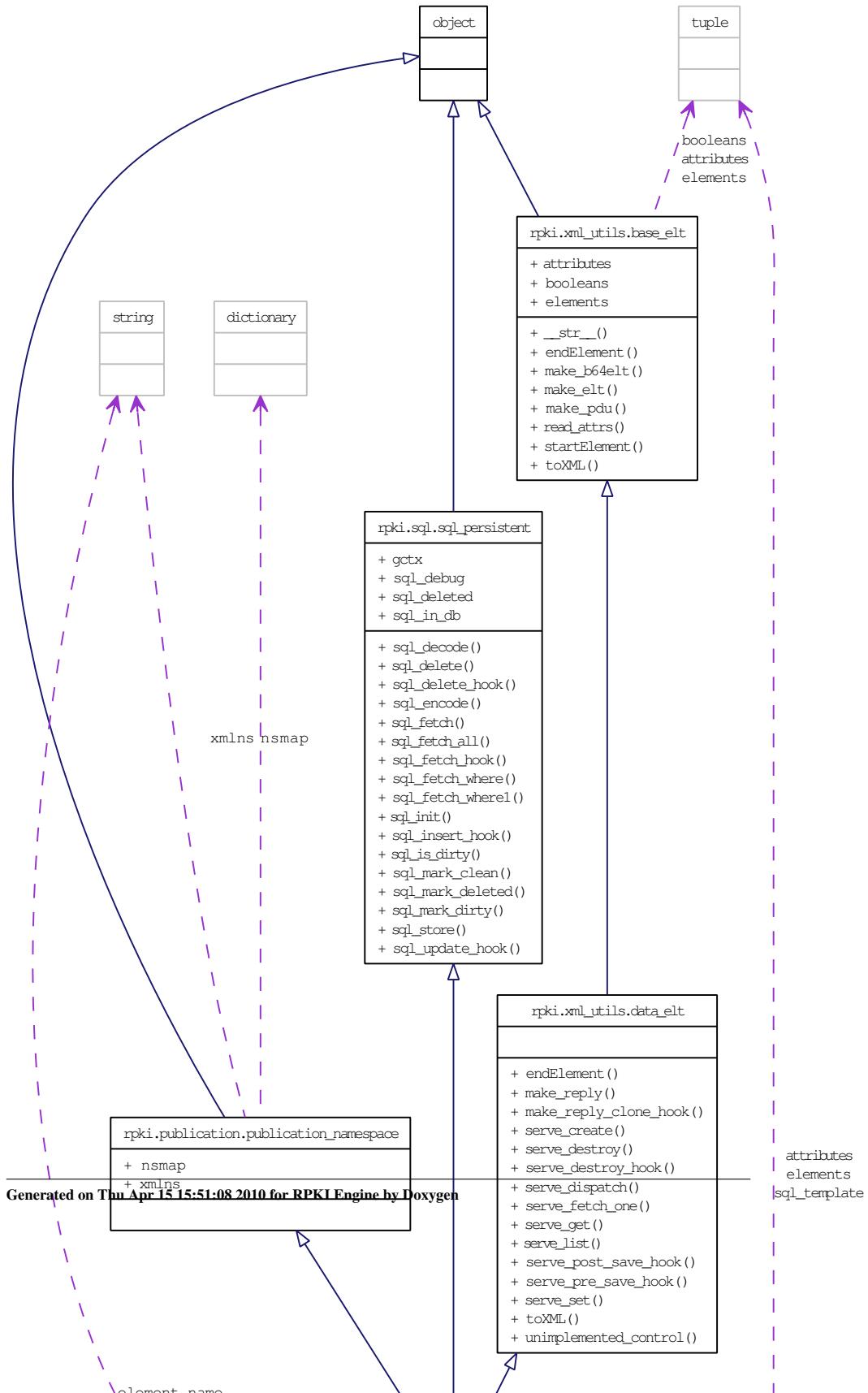
- `publication.py` (3107)

**11.133 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` = `rpk.sql.template("client", "client_id", "client_handle", "base_uri", ("bpxi_cert", rpk.x509.X509), ("bpxi_glue", rpk.x509.X509))`

#### 11.133.1 Detailed Description

<client/> element.

Definition at line 113 of file publication.py.

#### 11.133.2 Member Function Documentation

##### 11.133.2.1 def rpk.publication.client\_elt.check\_allowed\_uri (*self*, *uri*)

Definition at line 160 of file publication.py.

##### 11.133.2.2 def rpk.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.

### 11.133.2.3 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.

### 11.133.2.4 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.

### 11.133.2.5 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.

## 11.133.3 Member Data Documentation

### 11.133.3.1 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.

**11.133.3.2 rpki.publication.client\_elt.base\_uri = None [static]**

Definition at line 124 of file publication.py.

**11.133.3.3 rpki.publication.client\_elt.bpkı\_cert = None [static]**

Definition at line 125 of file publication.py.

**11.133.3.4 rpki.publication.client\_elt.bpkı\_glue = None [static]**

Definition at line 126 of file publication.py.

**11.133.3.5 rpki.publication.client\_elt.clear\_https\_ta\_cache = False [static]**

Definition at line 128 of file publication.py.

**11.133.3.6 string rpki.publication.client\_elt.element\_name = "client" [static]**

Definition at line 118 of file publication.py.

**11.133.3.7 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.

```
11.133.3.8 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:

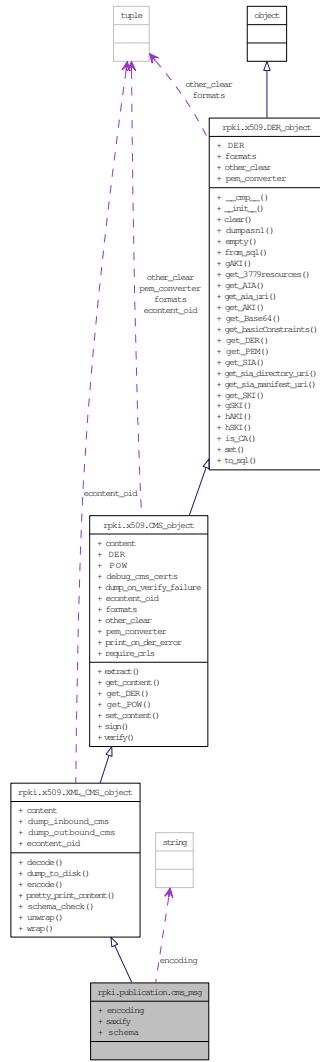
- [publication.py \(3107\)](#)

## 11.134 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`

### 11.134.1 Detailed Description

Class to hold a CMS-signed publication PDU.

Definition at line 415 of file publication.py.

### 11.134.2 Member Data Documentation

#### 11.134.2.1 string rpki.publication.cms\_msg.encoding = "us-ascii" [static]

Definition at line 420 of file publication.py.

#### 11.134.2.2 rpki.publication.cms\_msg.saxify = sax\_handler.saxify [static]

Reimplemented in [irbe\\_cli.publication\\_cms\\_msg](#).

Definition at line 422 of file publication.py.

#### 11.134.2.3 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:

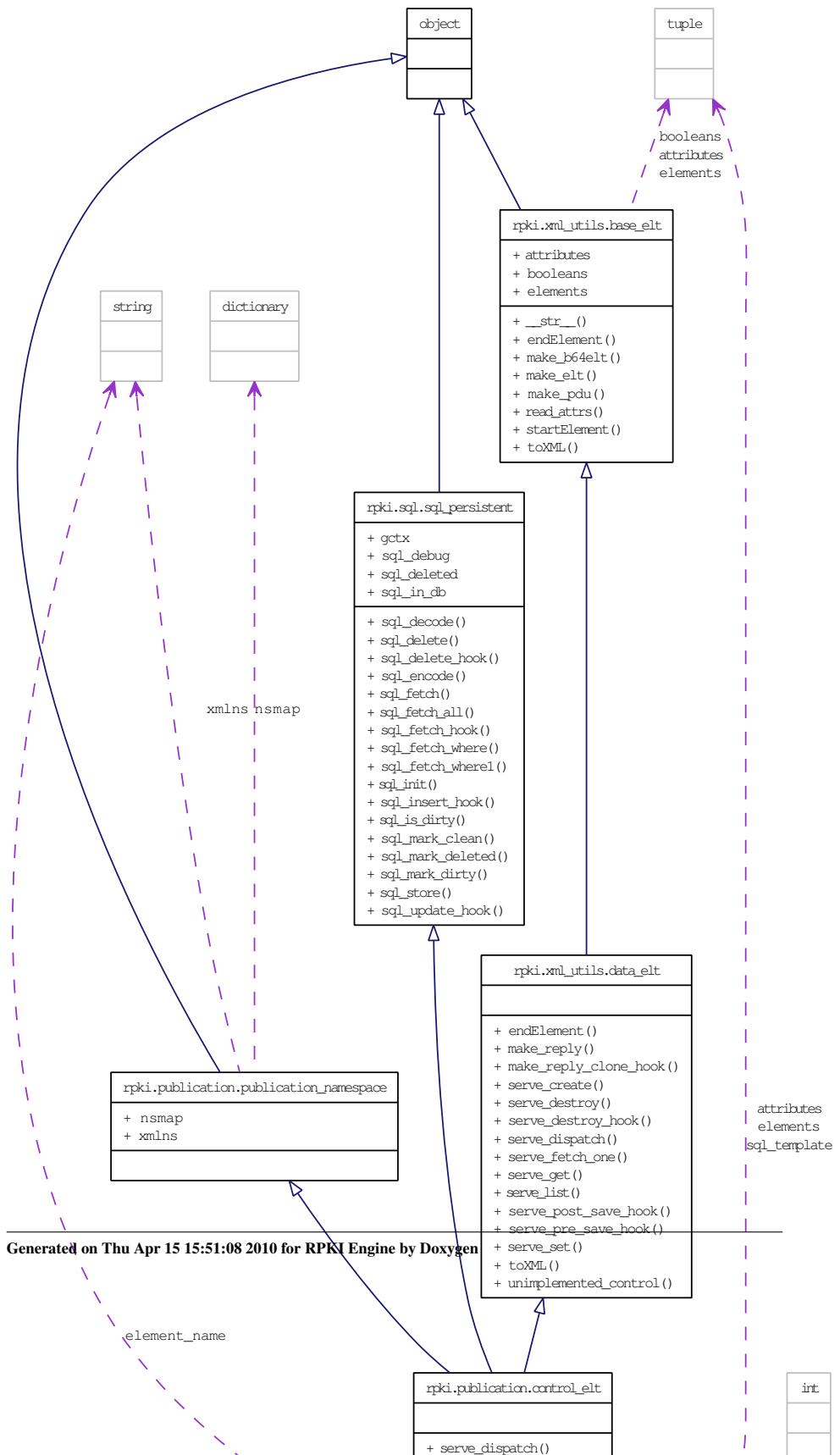
- [publication.py \(3107\)](#)

## 11.135 rpki.publication.config\_elt Class Reference

Inherits [rpki::publication::control\\_elt](#).

Inherited by [irbe\\_cli.config\\_elt](#).

## Collaboration diagram for rpki.publication.config\_elt:



### Public Member Functions

- def `fetch`
- def `serve_fetch_one_maybe`
- def `serve_set`
- def `startElement`

### Public Attributes

- `config_id`

### Static Public Attributes

- tuple `attributes` = ("action", "tag")  
*XML attributes for this element.*
- string `element_name` = "config"
- tuple `elements` = ("bpki\_crl",)  
*XML elements contained by this element.*
- tuple `sql_template` = `rpk.sql.template("config", "config_id", ("bpki_crl", rpk.x509.CRL))`
- int `wired_in_config_id` = 1

#### 11.135.1 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.

#### 11.135.2 Member Function Documentation

##### 11.135.2.1 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.

**11.135.2.2 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.

**11.135.2.3 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.

**11.135.2.4 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.

**11.135.3 Member Data Documentation****11.135.3.1 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.

**11.135.3.2 rpki.publication.config\_elt.config\_id**

Definition at line 86 of file publication.py.

**11.135.3.3 string rpki.publication.config\_elt.element\_name = "config"  
[static]**

Definition at line 73 of file publication.py.

**11.135.3.4 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.

**11.135.3.5 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.

**11.135.3.6 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:

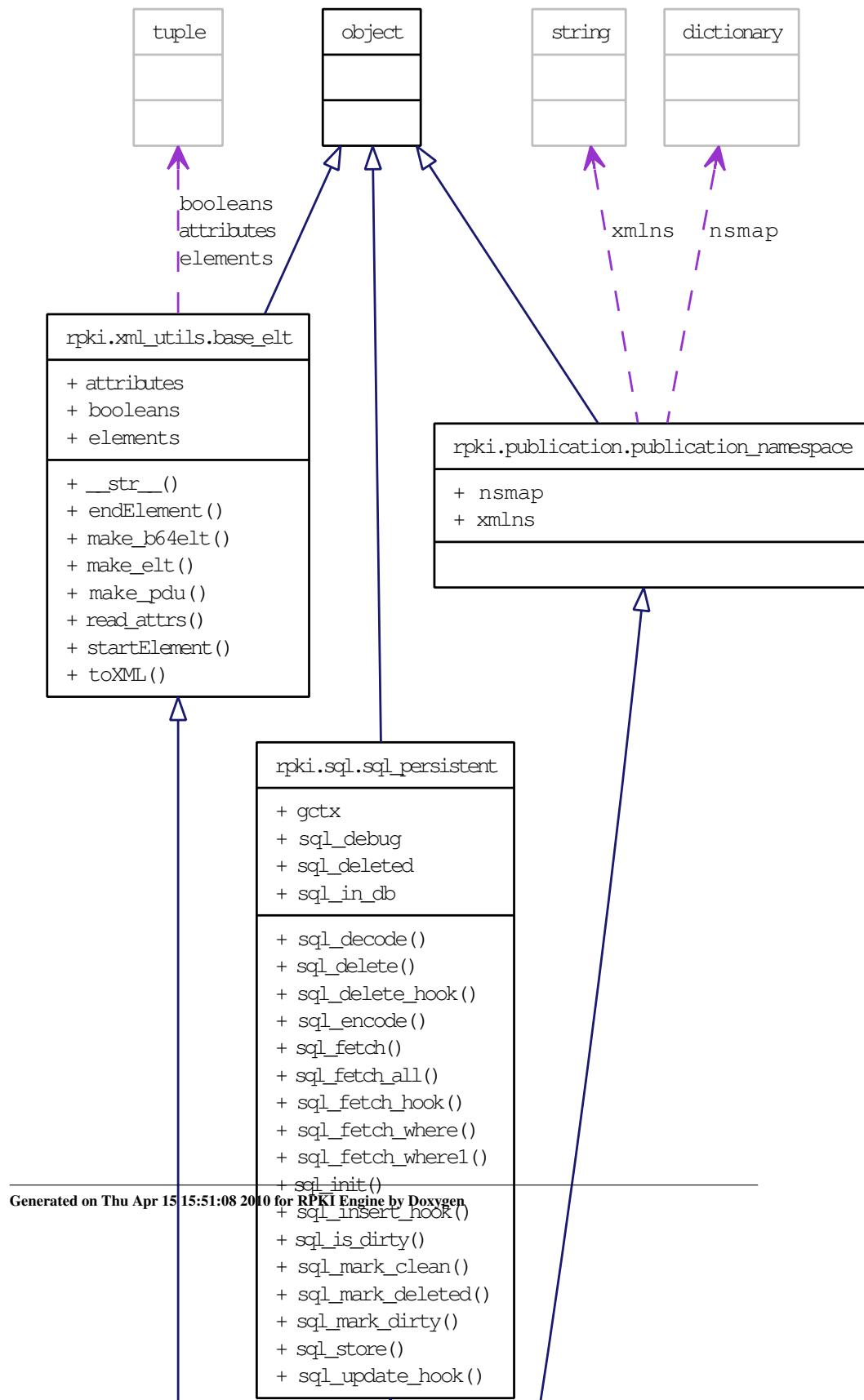
- [publication.py \(3107\)](#)

**11.136 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](#)

#### 11.136.1 Detailed Description

Virtual class for control channel objects.

Definition at line 47 of file publication.py.

#### 11.136.2 Member Function Documentation

##### 11.136.2.1 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:

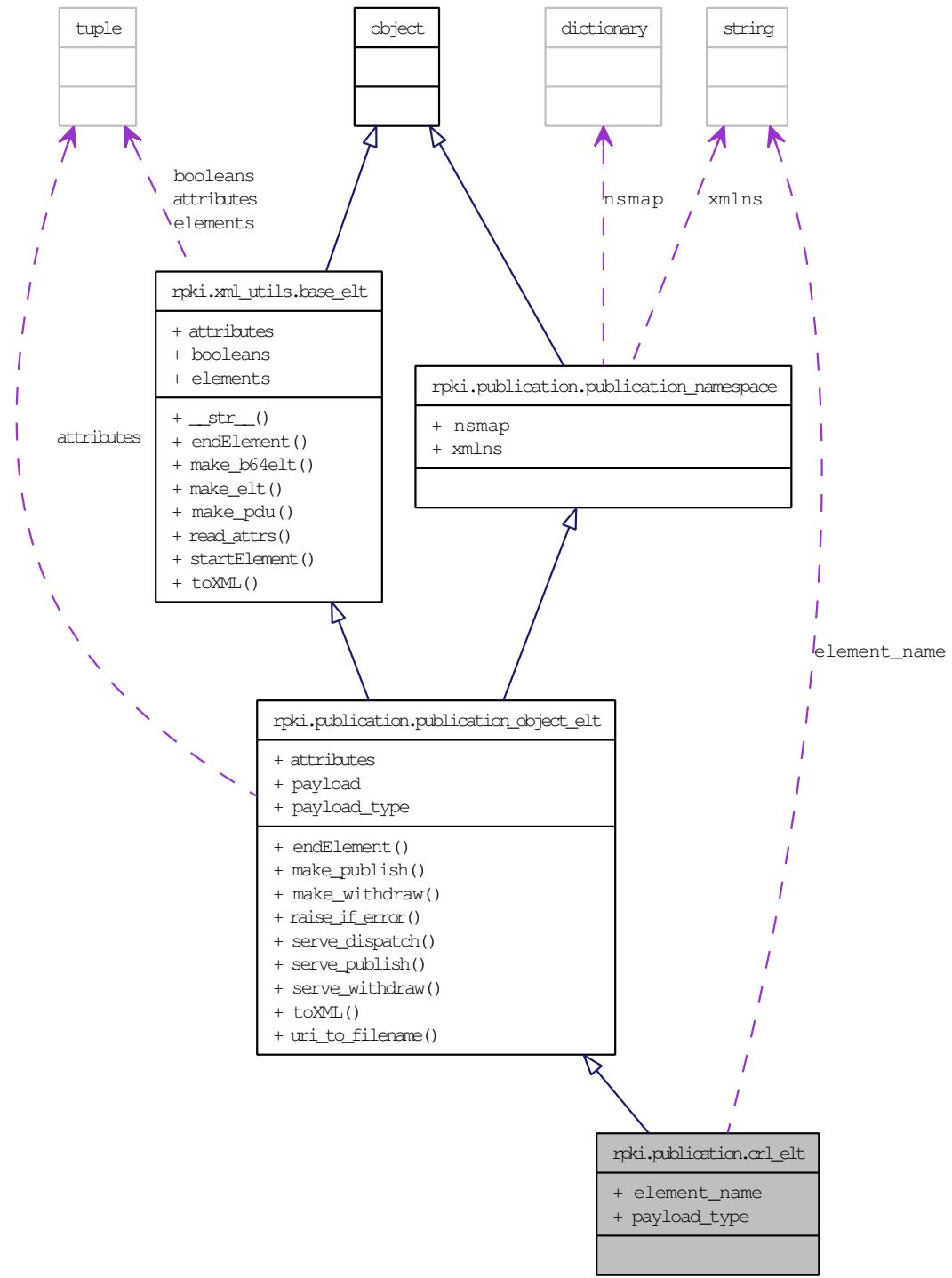
- [publication.py \(3107\)](#)

### 11.137 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` = `rpkি.x509.CRL`

#### 11.137.1 Detailed Description

`<crl/> element.`

Definition at line 295 of file publication.py.

#### 11.137.2 Member Data Documentation

##### 11.137.2.1 string rpkি.publication.crl\_elt.element\_name = "crl" [static]

Definition at line 300 of file publication.py.

##### 11.137.2.2 rpkি.publication.crl\_elt.payload\_type = rpkি.x509.CRL [static]

Reimplemented from `rpkি.publication.publication_object_elt`.

Definition at line 301 of file publication.py.

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

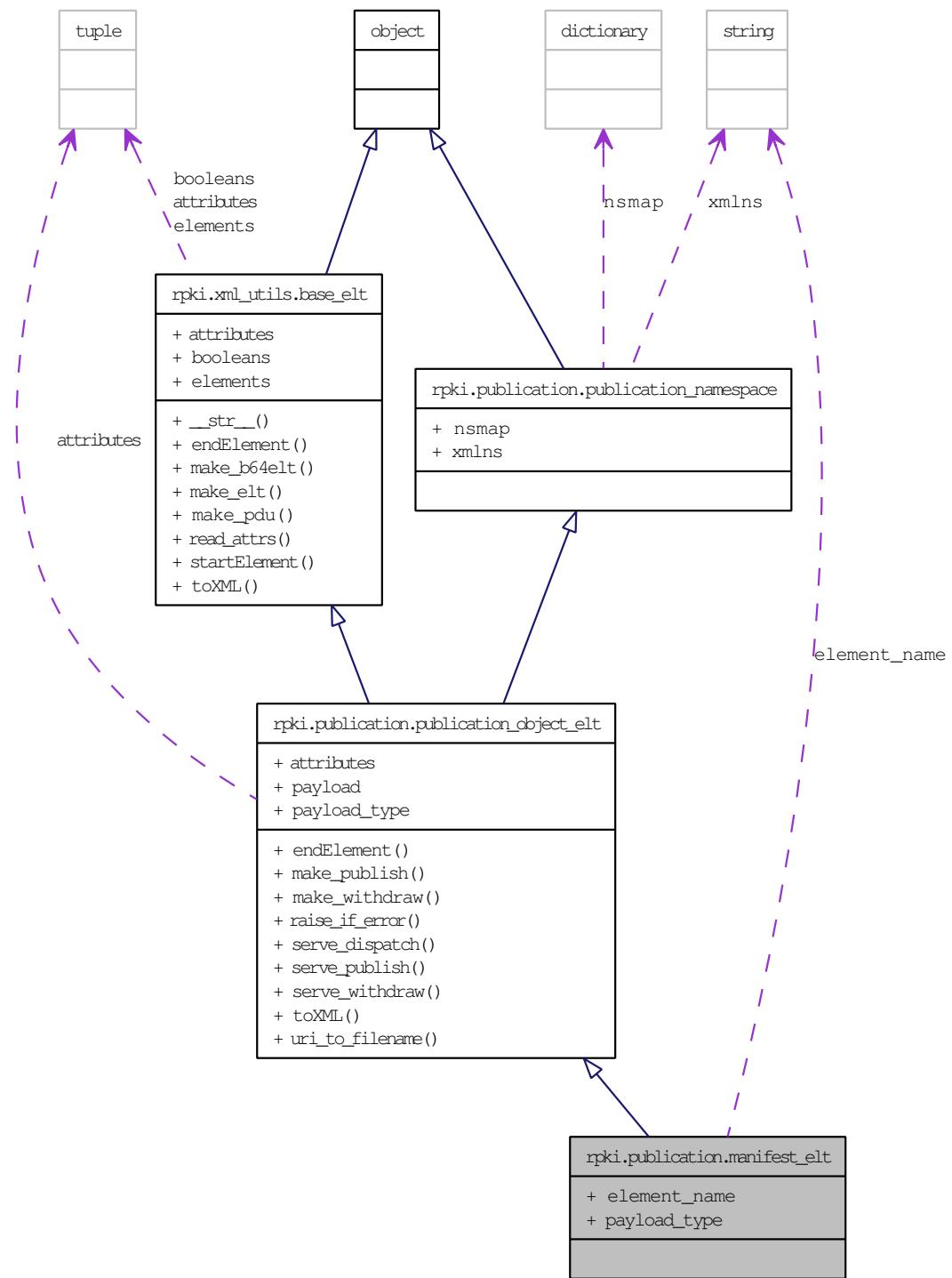
- `publication.py` (3107)

### 11.138 rpkি.publication.manifest\_elt Class Reference

Inherits `rpkি::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`

#### 11.138.1 Detailed Description

`<manifest/>` element.

Definition at line 303 of file publication.py.

#### 11.138.2 Member Data Documentation

##### 11.138.2.1 string `rpk.publication.manifest_elt.element_name` = "manifest" [static]

Definition at line 308 of file publication.py.

##### 11.138.2.2 `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:

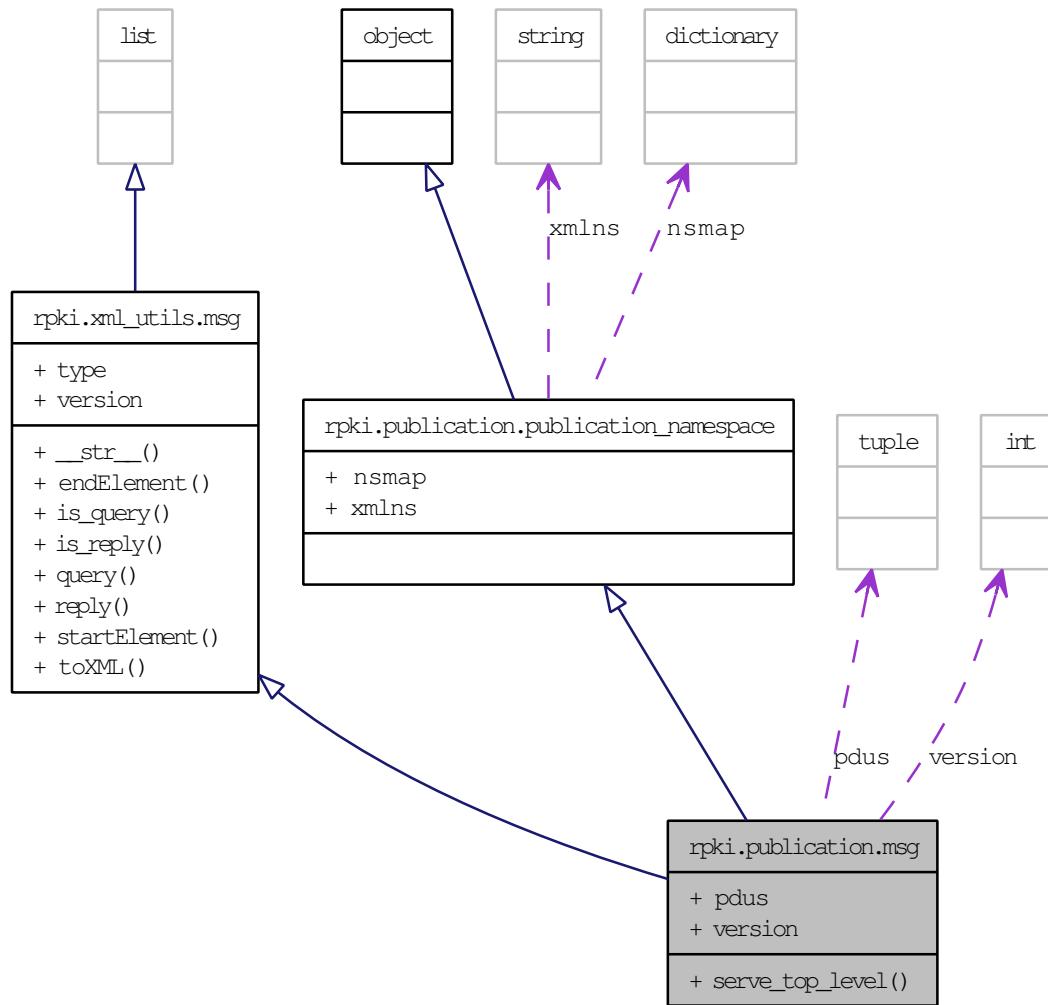
- `publication.py` (3107)

### 11.139 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.*

### 11.139.1 Detailed Description

Publication PDU.

Definition at line 362 of file publication.py.

### 11.139.2 Member Function Documentation

#### 11.139.2.1 def rpk.publication.msg.serve\_top\_level ( *self*, *gctx*, *client*, *cb* )

Serve one msg PDU.

Definition at line 376 of file publication.py.

### 11.139.3 Member Data Documentation

#### 11.139.3.1 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.

#### 11.139.3.2 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:

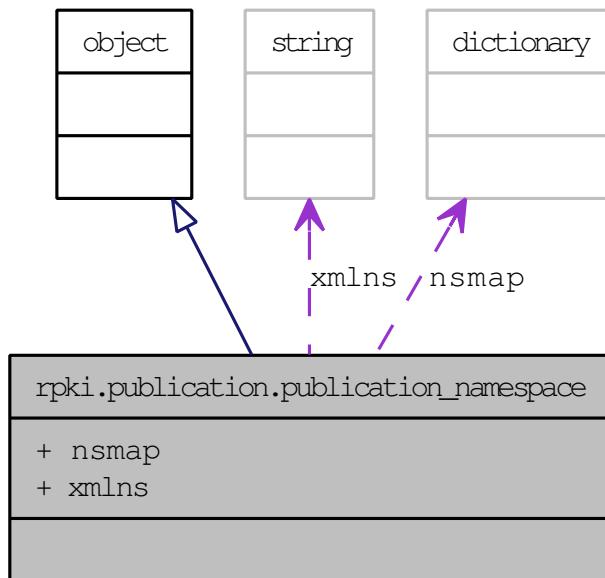
- publication.py (3107)

## 11.140 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/"

#### 11.140.1 Detailed Description

XML namespace parameters for publication protocol.

Definition at line 39 of file publication.py.

### 11.140.2 Member Data Documentation

**11.140.2.1** `dictionary rPKI.publication.publication_namespace.nsmap = { None : xmlns } [static]`

Definition at line 45 of file publication.py.

**11.140.2.2** `string rPKI.publication.publication_namespace.xmlns = "http://www.hactrn.net/uris/rPKI/publication-spec/" [static]`

Definition at line 44 of file publication.py.

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

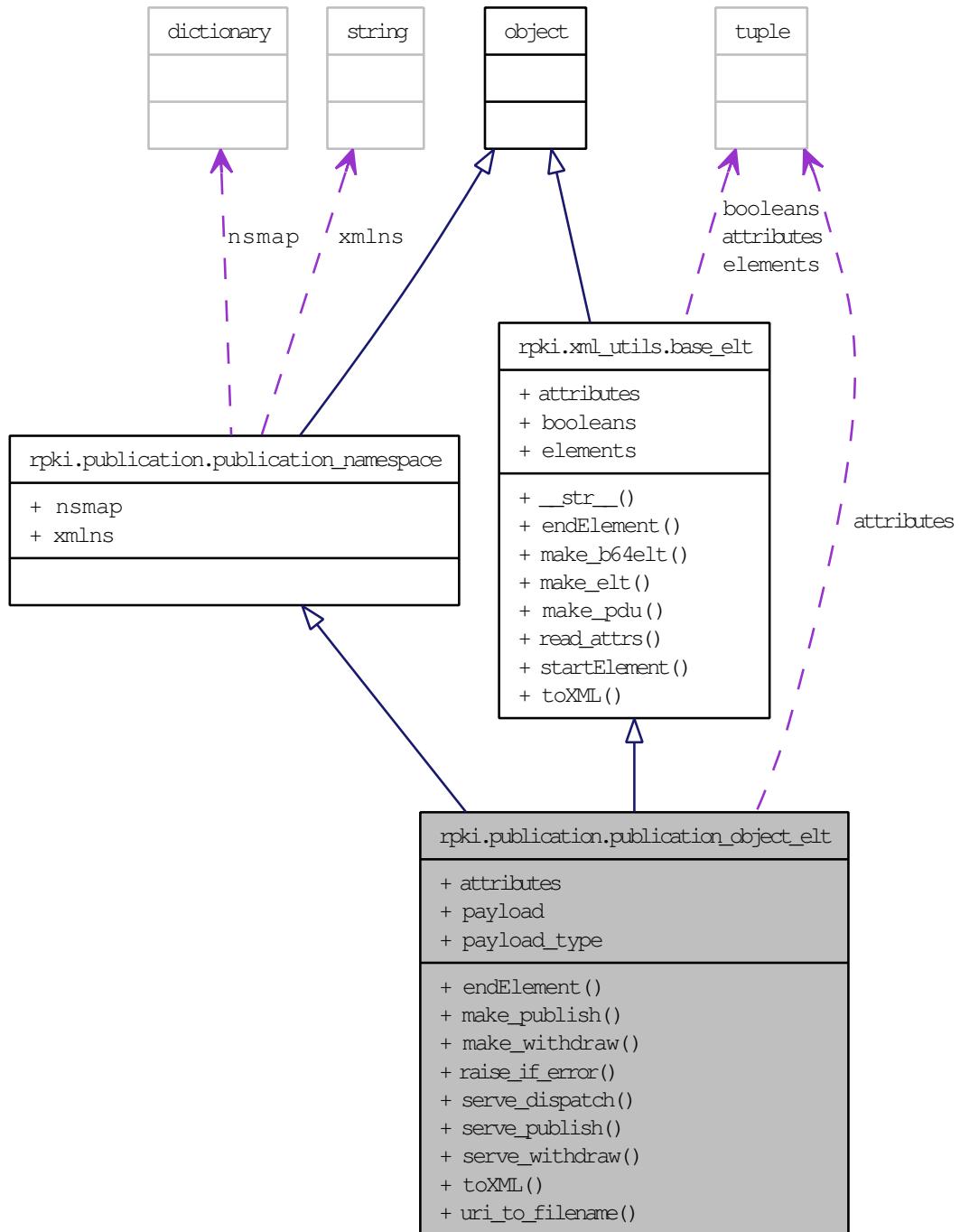
- [publication.py \(3107\)](#)

## 11.141 rPKI.publication.publication\_object\_elt Class Reference

Inherits [rPKI::xml\\_utils::base\\_elt](#), and [rPKI::publication::publication\\_namespace](#).

Inherited by [rPKI.publication.certificate\\_elt](#), [rPKI.publication.crl\\_elt](#), [rPKI.publication.manifest\\_elt](#), and [rPKI.publication.roa\\_elt](#).

Collaboration diagram for 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

#### 11.141.1 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.

#### 11.141.2 Member Function Documentation

##### 11.141.2.1 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.

**11.141.2.2 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.

**11.141.2.3 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.

**11.141.2.4 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.

**11.141.2.5 def rpkি.publication.publication\_object\_elt.serve\_dispatch ( *self*,  
*r\_msg*, *cb*, *eb*)**

Action dispatch handler.

Definition at line 196 of file publication.py.

**11.141.2.6 def rpkি.publication.publication\_object\_elt.serve\_publish ( *self*)**

Publish an object.

Definition at line 221 of file publication.py.

**11.141.2.7 def rpk.publication.publication\_object\_elt.serve\_withdraw ( *self* )**

Withdraw an object.

Definition at line 236 of file publication.py.

**11.141.2.8 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.

**11.141.2.9 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.

**11.141.3 Member Data Documentation****11.141.3.1 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.

**11.141.3.2 rpk.publication.publication\_object\_elt.payload = None [static]**

Definition at line 176 of file publication.py.

**11.141.3.3 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:

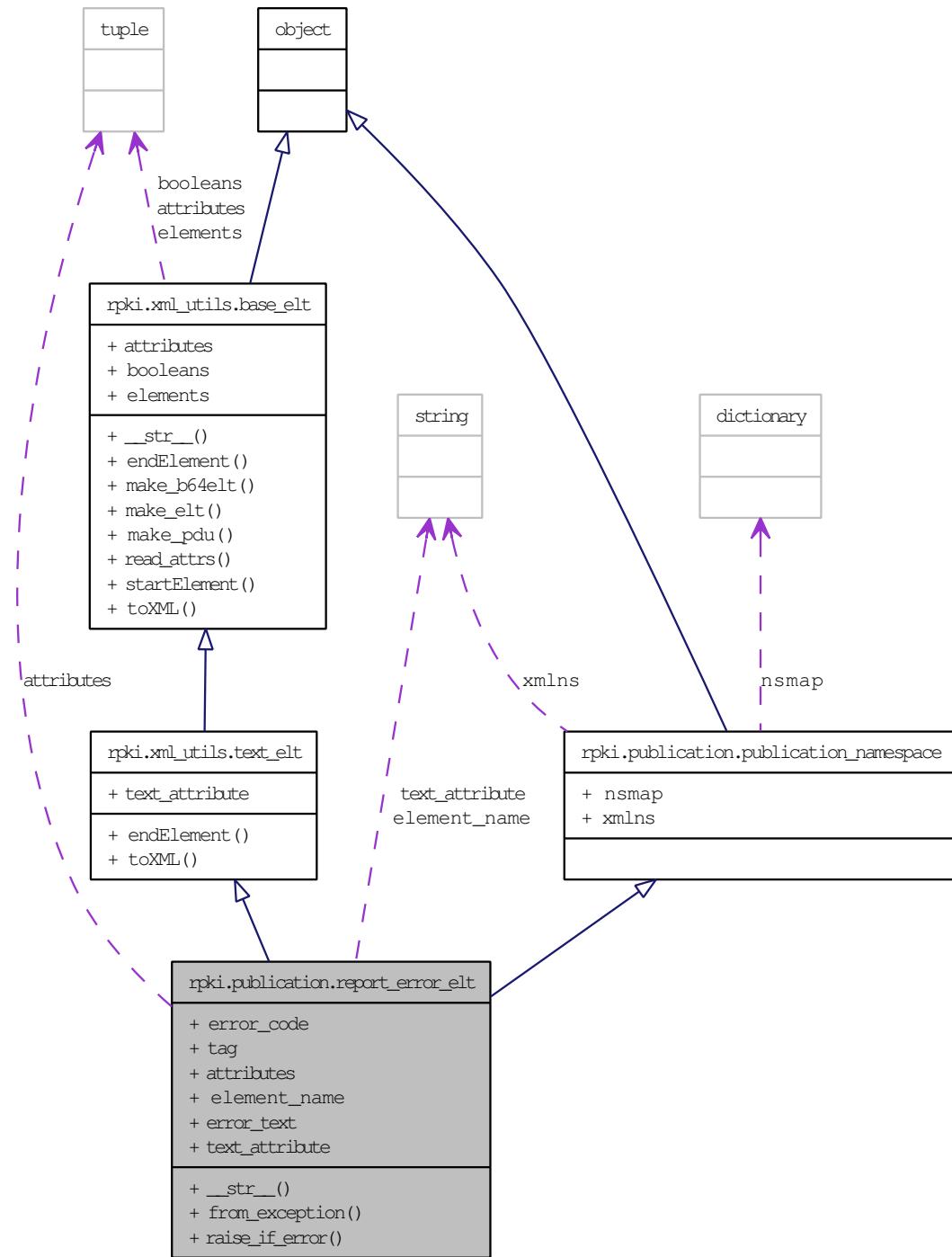
- [publication.py \(3107\)](#)

**11.142 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.*

### 11.142.1 Detailed Description

<report\_error/> element.

Definition at line 321 of file publication.py.

### 11.142.2 Member Function Documentation

#### 11.142.2.1 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.

**11.142.2.2 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.

**11.142.2.3 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.

**11.142.3 Member Data Documentation****11.142.3.1 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.

**11.142.3.2 string rpki.publication.report\_error\_elt.element\_name = "report\_error" [static]**

Definition at line 326 of file publication.py.

**11.142.3.3 rpki.publication.report\_error\_elt.error\_code**

Definition at line 339 of file publication.py.

**11.142.3.4 rpki.publication.report\_error\_elt.error\_text = None [static]**

Definition at line 330 of file publication.py.

**11.142.3.5 rpki.publication.report\_error\_elt.tag**

Definition at line 338 of file publication.py.

**11.142.3.6 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:

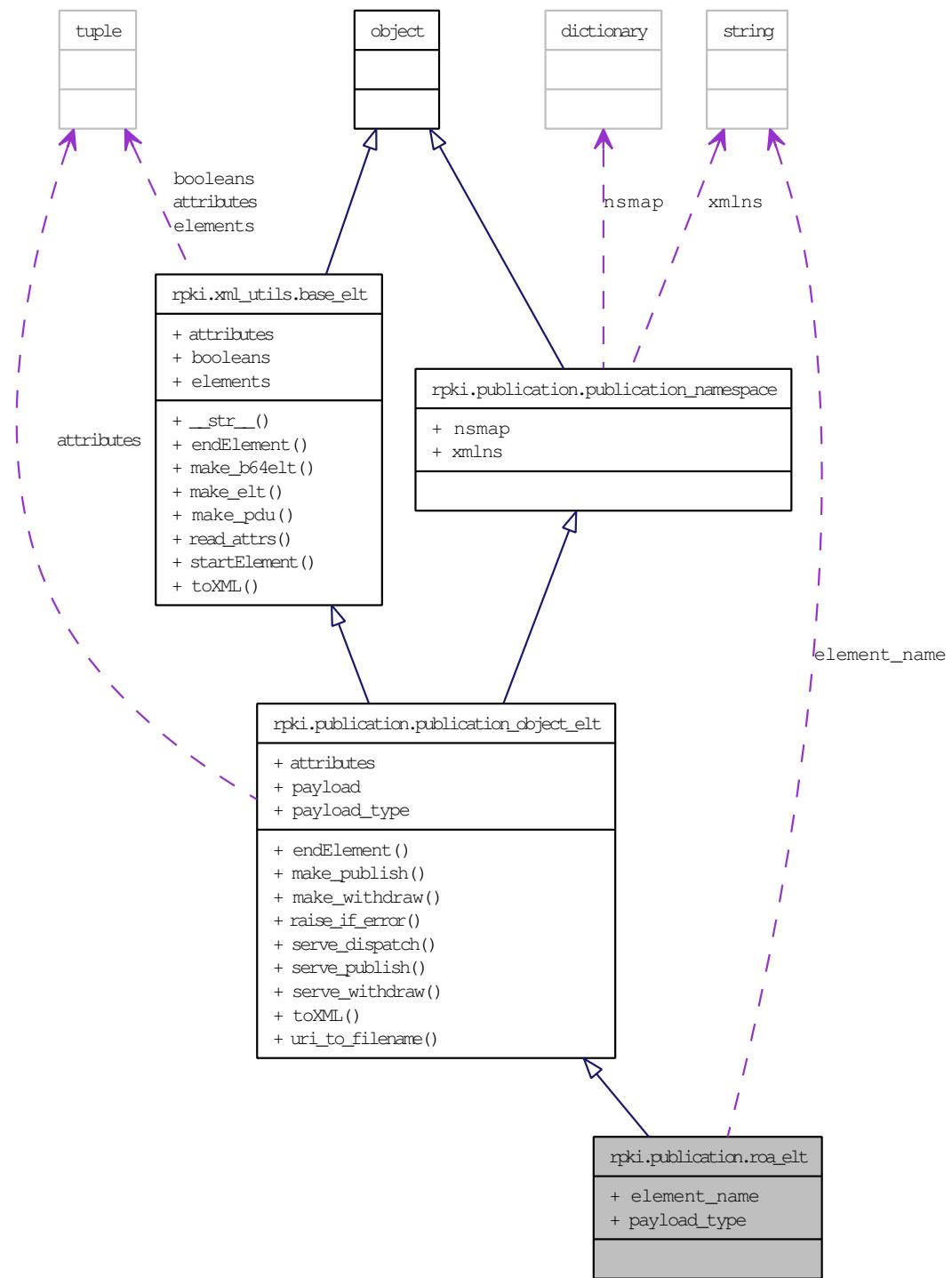
- [publication.py \(3107\)](#)

**11.143 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`

#### 11.143.1 Detailed Description

`<roa/>` element.

Definition at line 311 of file publication.py.

#### 11.143.2 Member Data Documentation

##### 11.143.2.1 string `rpkি.publication.roa_elt.element_name` = "roa" [static]

Definition at line 316 of file publication.py.

##### 11.143.2.2 `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:

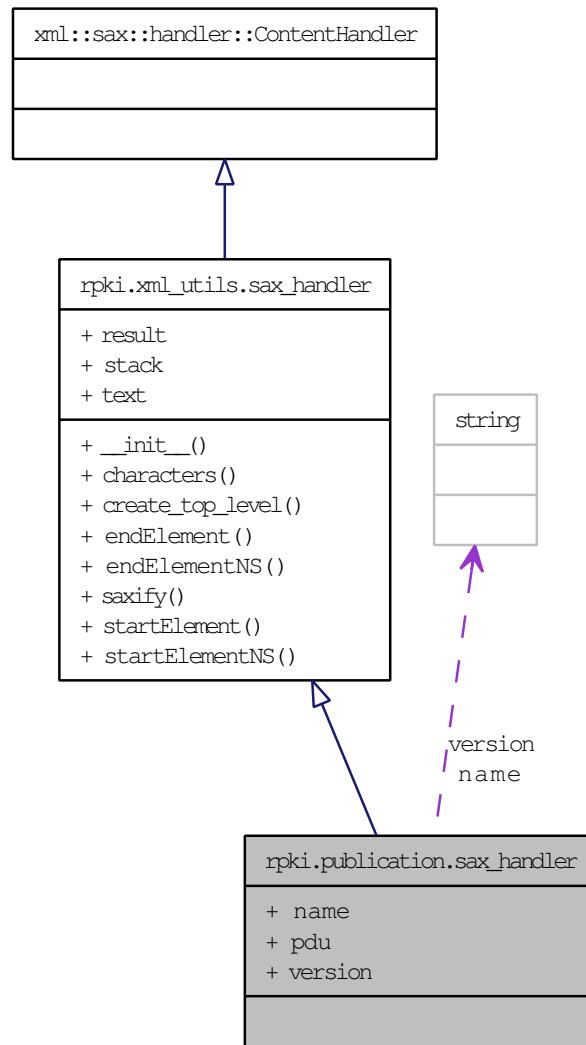
- `publication.py` (3107)

## 11.144 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"

### 11.144.1 Detailed Description

SAX handler for publication protocol.

Definition at line 406 of file publication.py.

### 11.144.2 Member Data Documentation

#### 11.144.2.1 string rpkি.publication.sax\_handler.name = "msg" [static]

Definition at line 412 of file publication.py.

#### 11.144.2.2 rpkি.publication.sax\_handler.pdu = msg [static]

Reimplemented in [irbe\\_cli.publication\\_sax\\_handler](#).

Definition at line 411 of file publication.py.

#### 11.144.2.3 string rpkি.publication.sax\_handler.version = "1" [static]

Definition at line 413 of file publication.py.

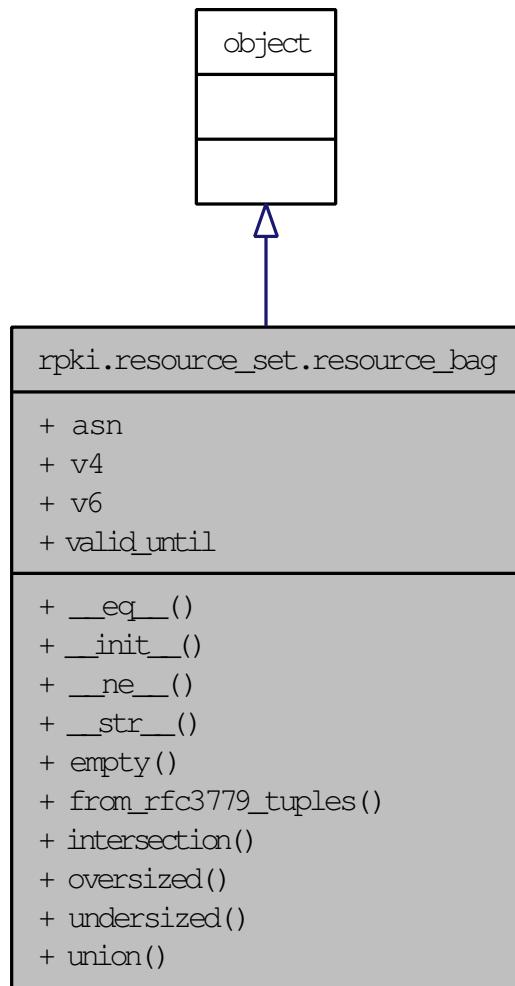
The documentation for this class was generated from the following file:

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

## 11.145 rpkি.resource\_set.resource\_bag Class Reference

Inherits [object](#).

Collaboration diagram for rpkি.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.*

### 11.145.1 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.

### 11.145.2 Member Function Documentation

#### 11.145.2.1 def rpkি.resource\_set.resource\_bag.\_\_eq\_\_(self, other)

Definition at line 615 of file resource\_set.py.

#### 11.145.2.2 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.

**11.145.2.3 def rpkি.resource\_set.resource\_bag.\_\_ne\_\_ (*self*, *other*)**

Definition at line 621 of file resource\_set.py.

**11.145.2.4 def rpkি.resource\_set.resource\_bag.\_\_str\_\_ (*self*)**

Definition at line 644 of file resource\_set.py.

**11.145.2.5 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.

**11.145.2.6 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.

**11.145.2.7 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.

**11.145.2.8 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.

**11.145.2.9 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.

**11.145.2.10 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.

**11.145.3 Member Data Documentation****11.145.3.1 rpkি::resource\_set.resource\_bag::asn**

Set of Autonomous System Number resources.

Definition at line 566 of file resource\_set.py.

**11.145.3.2 rpkি::resource\_set.resource\_bag::v4**

Set of IPv4 resources.

Definition at line 567 of file resource\_set.py.

**11.145.3.3 rpkি::resource\_set.resource\_bag::v6**

Set of IPv6 resources.

Definition at line 568 of file resource\_set.py.

**11.145.3.4 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:

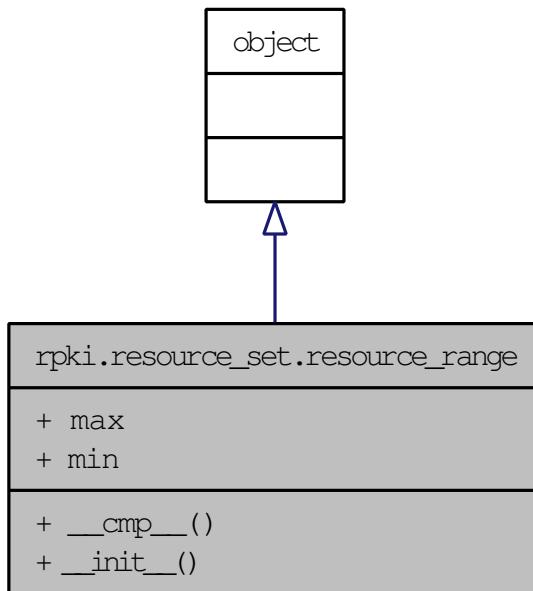
- [resource\\_set.py \(3107\)](#)

## 11.146 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](#)

### 11.146.1 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`.

### 11.146.2 Member Function Documentation

#### 11.146.2.1 def rpkি.resource\_set.resource\_range.\_\_cmp\_\_ (*self, other*)

Compare two `resource_range` objects.

Definition at line 67 of file `resource_set.py`.

#### 11.146.2.2 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`.

### 11.146.3 Member Data Documentation

#### 11.146.3.1 rpkি.resource\_set.resource\_range.max

Definition at line 65 of file `resource_set.py`.

#### 11.146.3.2 rpkি.resource\_set.resource\_range.min

Reimplemented in [rpkি.resource\\_set.resource\\_range\\_as](#).

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

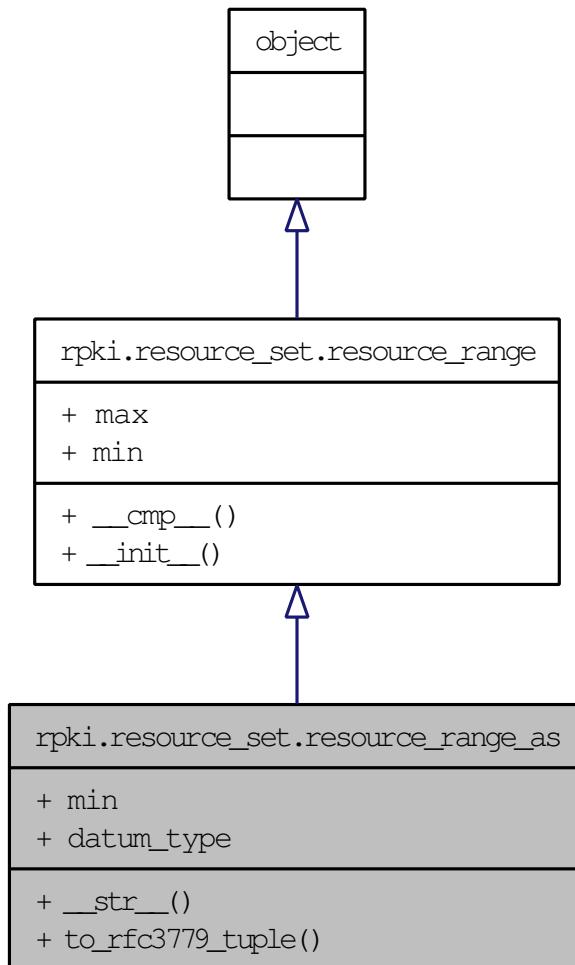
The documentation for this class was generated from the following file:

- [resource\\_set.py \(3107\)](#)

## 11.147 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).*

## 11.147.1 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.

## 11.147.2 Member Function Documentation

### 11.147.2.1 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.

### 11.147.2.2 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.

## 11.147.3 Member Data Documentation

### 11.147.3.1 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.

### **11.147.3.2 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:

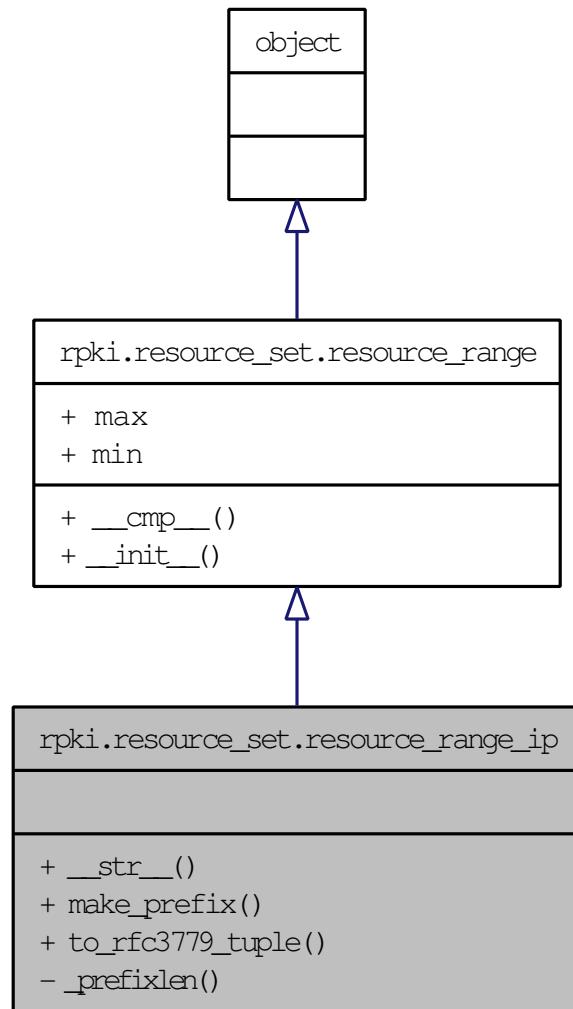
- [resource\\_set.py \(3107\)](#)

## **11.148 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 rPKI.resource\_set.resource\_range\_ip:



### Public Member Functions

- def `__str__`
- def `make_prefix`
- def `to_rfc3779_tuple`

### Private Member Functions

- def [\\_prefixlen](#)

#### 11.148.1 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.

#### 11.148.2 Member Function Documentation

##### 11.148.2.1 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.

##### 11.148.2.2 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.

##### 11.148.2.3 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.

**11.148.2.4 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.

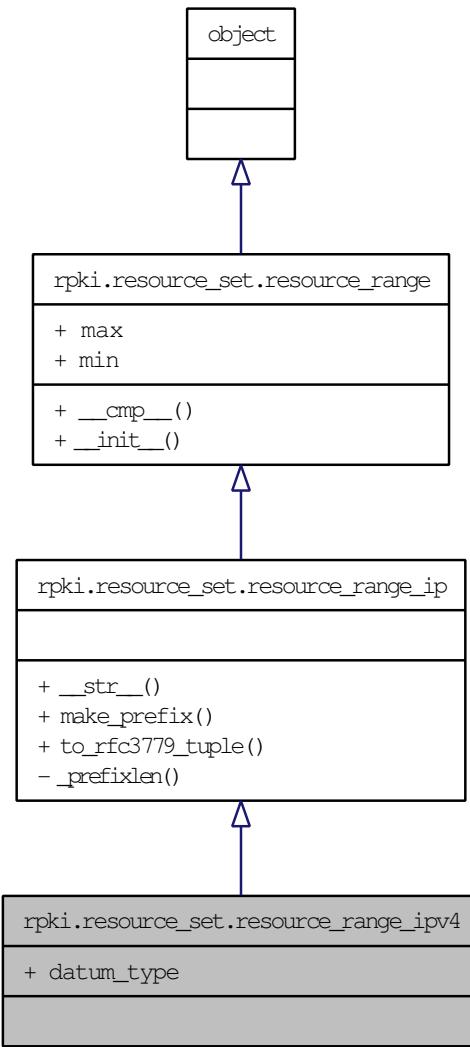
The documentation for this class was generated from the following file:

- [resource\\_set.py \(3107\)](#)

**11.149 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).*

### **11.149.1 Detailed Description**

Range of IPv4 addresses.

Definition at line 170 of file resource\_set.py.

### **11.149.2 Member Data Documentation**

#### **11.149.2.1 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.

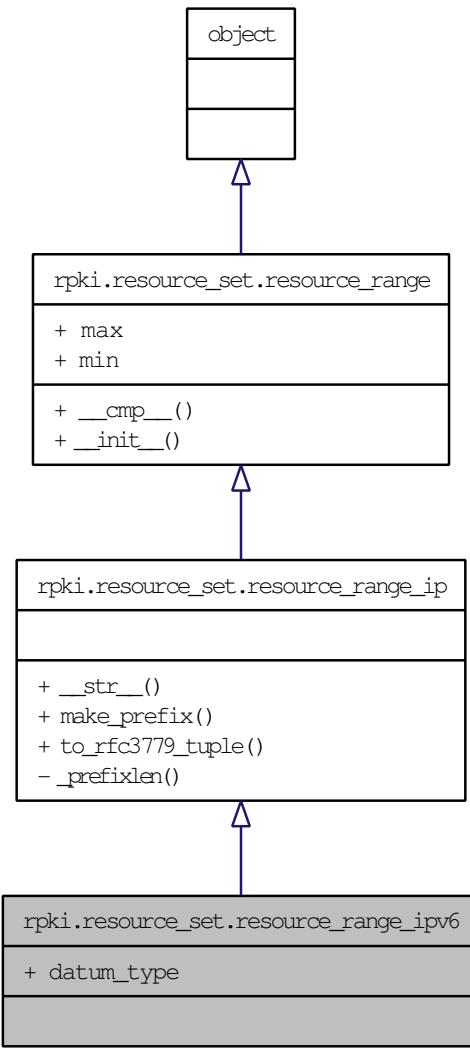
The documentation for this class was generated from the following file:

- [resource\\_set.py \(3107\)](#)

## **11.150 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).*

### **11.150.1 Detailed Description**

Range of IPv6 addresses.

Definition at line 180 of file resource\_set.py.

### **11.150.2 Member Data Documentation**

#### **11.150.2.1 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:

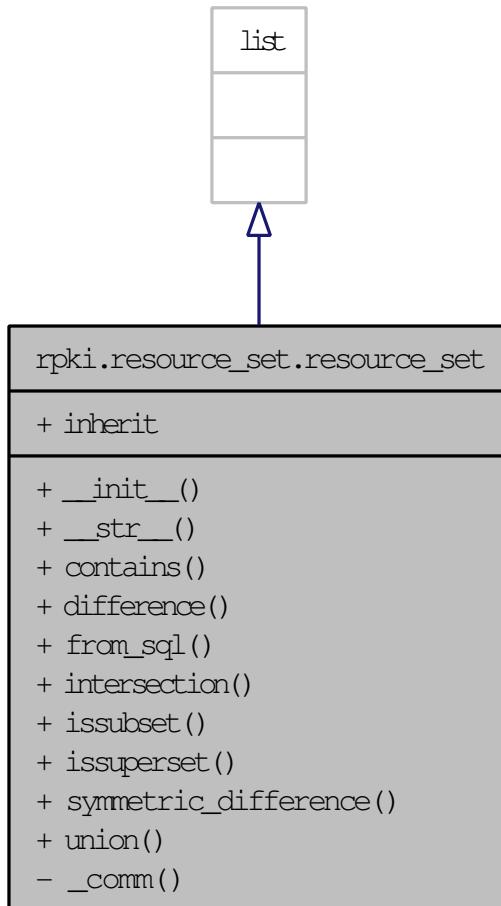
- [resource\\_set.py \(3107\)](#)

## **11.151 rpki.resource\_set.resource\_set Class Reference**

Inherits list.

Inherited by [rpki.resource\\_set.resource\\_set\\_as](#), and [rpki.resource\\_set.resource\\_set\\_ip](#).

Collaboration diagram for rPKI.resource\_set.resource\_set:



### Public Member Functions

- def \_\_init\_\_
- def \_\_str\_\_
- def contains
- def difference
- def from\_sql
- def intersection
- def issubset
- def issuperset
- def symmetric\_difference
- def union

### Static Public Attributes

- `inherit` = False

*Boolean indicating whether this `resource_set` uses RFC 3779 inheritance.*

### Private Member Functions

- `def _comm`

#### 11.151.1 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`.

#### 11.151.2 Member Function Documentation

##### 11.151.2.1 def rpkি.resource\_set.resource\_set.\_\_init\_\_ (`self`, `ini = None`)

Initialize a `resource_set`.

Definition at line 219 of file `resource_set.py`.

##### 11.151.2.2 def rpkি.resource\_set.resource\_set.\_\_str\_\_ (`self`)

Convert a `resource_set` to string format.

Definition at line 246 of file `resource_set.py`.

##### 11.151.2.3 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.

#### 11.151.2.4 def rpkি.resource\_set.resource\_set.contains (*self, item*)

Set membership test for resource sets.

Definition at line 332 of file resource\_set.py.

#### 11.151.2.5 def rpkি.resource\_set.resource\_set.difference (*self, other*)

Set difference for resource sets.

Definition at line 323 of file resource\_set.py.

#### 11.151.2.6 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.

#### 11.151.2.7 def rpkি.resource\_set.resource\_set.intersection (*self, other*)

Set intersection for resource sets.

Definition at line 319 of file resource\_set.py.

**11.151.2.8 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.

**11.151.2.9 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.

**11.151.2.10 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.

**11.151.2.11 def rpkি.resource\_set.resource\_set.union (*self*, *other*)**

Set union for resource sets.

Definition at line 288 of file resource\_set.py.

**11.151.3 Member Data Documentation****11.151.3.1 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.

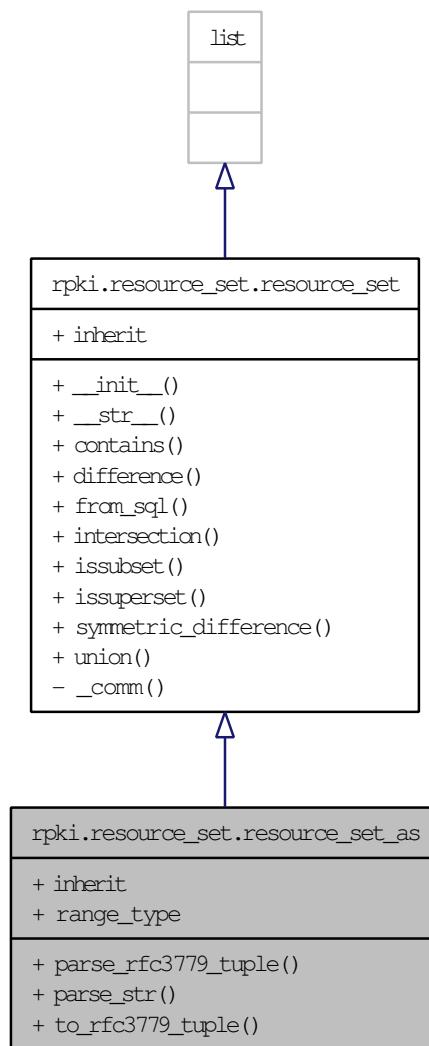
The documentation for this class was generated from the following file:

- [resource\\_set.py \(3107\)](#)

## 11.152 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](#).*

#### 11.152.1 Detailed Description

Autonomous System Number resource set.

Definition at line 384 of file [resource\\_set.py](#).

#### 11.152.2 Member Function Documentation

##### 11.152.2.1 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](#).

##### 11.152.2.2 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](#).

**11.152.2.3 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.

**11.152.3 Member Data Documentation****11.152.3.1 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.

**11.152.3.2 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:

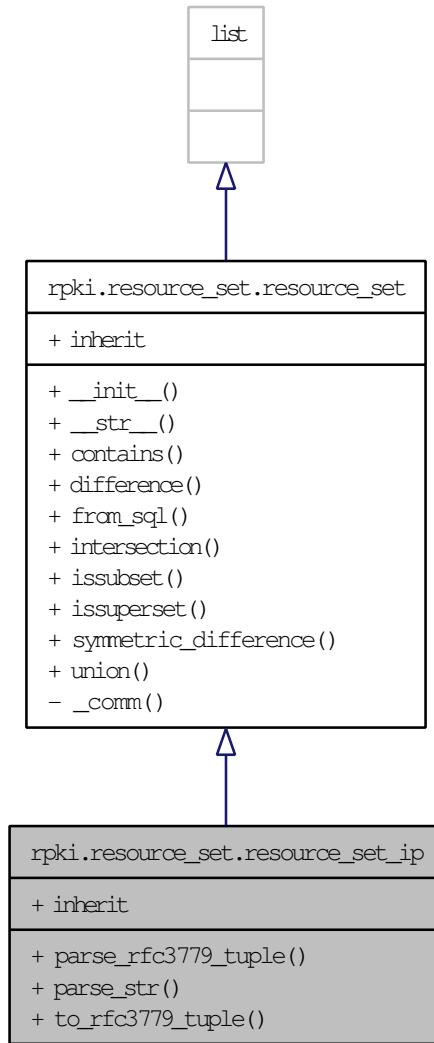
- [resource\\_set.py \(3107\)](#)

**11.153 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.*

### 11.153.1 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`.

### 11.153.2 Member Function Documentation

#### 11.153.2.1 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`.

#### 11.153.2.2 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`.

#### 11.153.2.3 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`.

### 11.153.3 Member Data Documentation

#### 11.153.3.1 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](#).

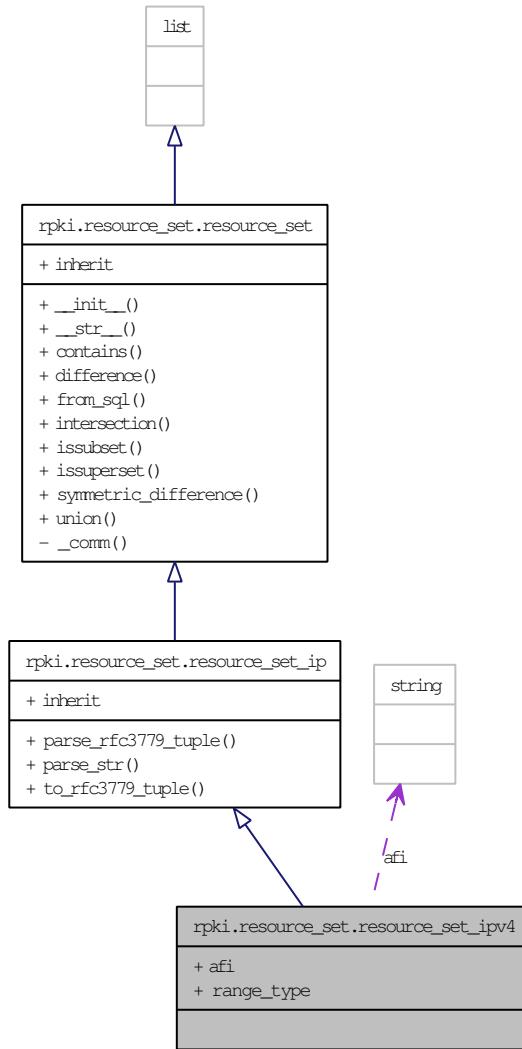
The documentation for this class was generated from the following file:

- [resource\\_set.py \(3107\)](#)

## 11.154 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](#).*

### 11.154.1 Detailed Description

IPv4 address resource set.

Definition at line 484 of file resource\_set.py.

### 11.154.2 Member Data Documentation

#### 11.154.2.1 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.

#### 11.154.2.2 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.

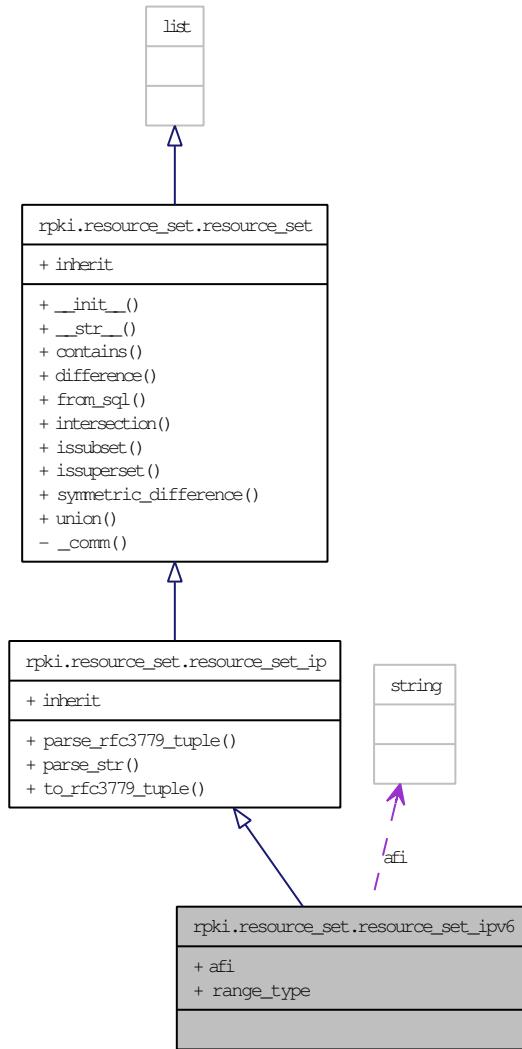
The documentation for this class was generated from the following file:

- [resource\\_set.py \(3107\)](#)

## 11.155 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`.*

### 11.155.1 Detailed Description

IPv6 address resource set.

Definition at line 499 of file `resource_set.py`.

### 11.155.2 Member Data Documentation

#### 11.155.2.1 `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`.

#### 11.155.2.2 `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:

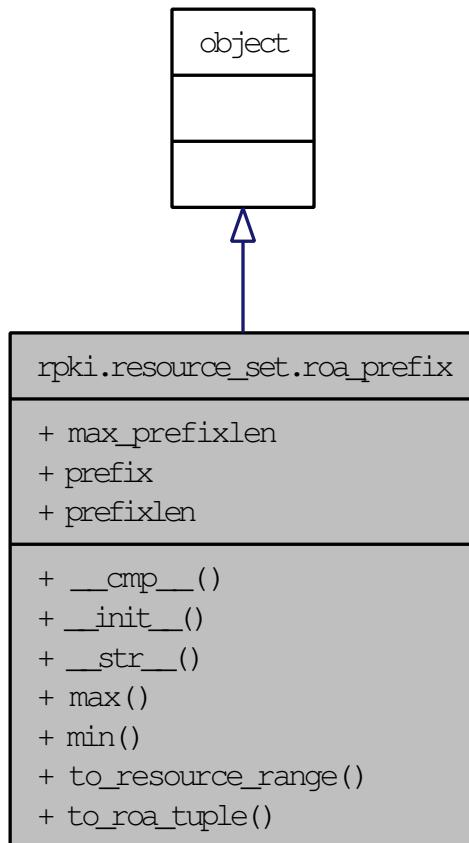
- [resource\\_set.py \(3107\)](#)

## 11.156 rpkি.resource\_set.roa\_prefix Class Reference

Inherits [object](#).

Inherited by [rpkি.resource\\_set.roa\\_prefix\\_ipv4](#), and [rpkি.resource\\_set.roa\\_prefix\\_ipv6](#).

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.*

### 11.156.1 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.

### 11.156.2 Member Function Documentation

#### 11.156.2.1 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.

#### 11.156.2.2 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.

#### 11.156.2.3 def rpkি.resource\_set.roa\_prefix.\_\_str\_\_ ( self)

Convert a ROA prefix to string format.

Definition at line 710 of file resource\_set.py.

**11.156.2.4 def rpkি.resource\_set.roa\_prefix.max ( *self* )**

Return highest address covered by prefix.

Definition at line 731 of file resource\_set.py.

**11.156.2.5 def rpkি.resource\_set.roa\_prefix.min ( *self* )**

Return lowest address covered by prefix.

Definition at line 727 of file resource\_set.py.

**11.156.2.6 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.

**11.156.2.7 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.

**11.156.3 Member Data Documentation****11.156.3.1 rpkি::resource\_set.roa\_prefix::max\_prefixlen**

Maxmimum prefix length.

Definition at line 695 of file resource\_set.py.

**11.156.3.2 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.

**11.156.3.3 rpkি::resource\_set.roa\_prefix::prefixlen**

(Minimum) prefix length.

Definition at line 694 of file resource\_set.py.

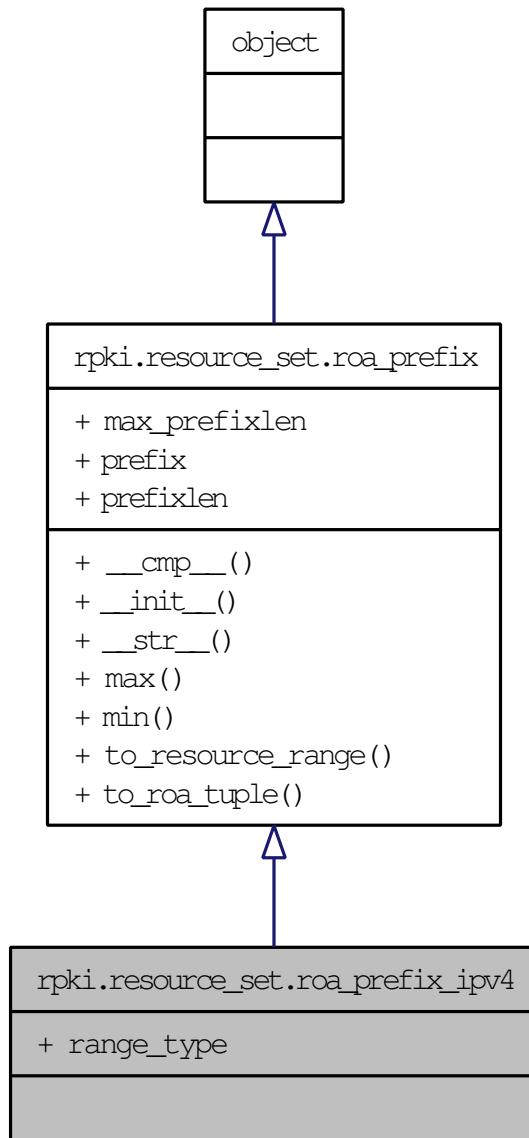
The documentation for this class was generated from the following file:

- [resource\\_set.py \(3107\)](#)

**11.157 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`.*

### **11.157.1 Detailed Description**

IPv4 ROA prefix.

Definition at line 746 of file resource\_set.py.

### **11.157.2 Member Data Documentation**

#### **11.157.2.1 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.

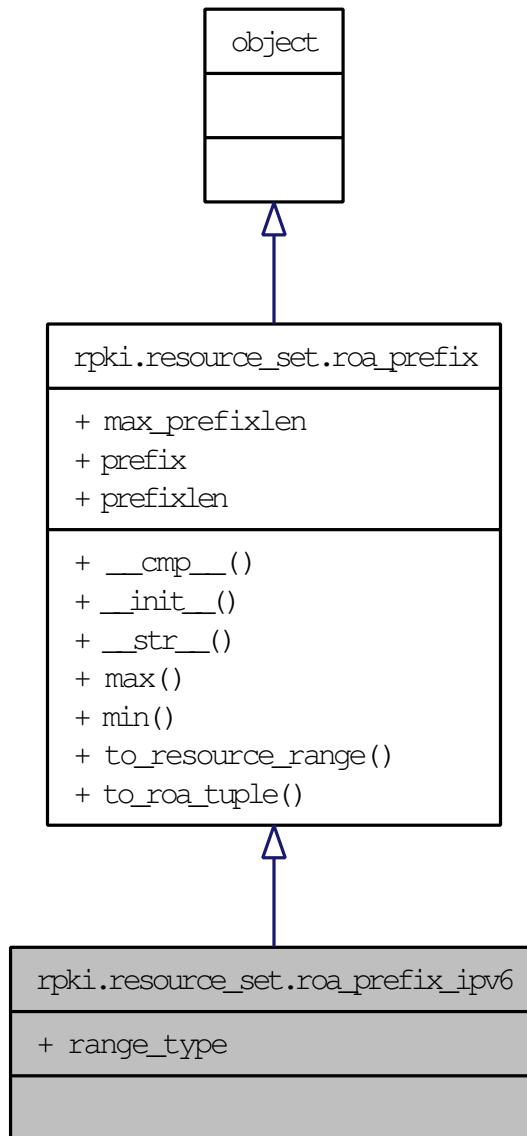
The documentation for this class was generated from the following file:

- [resource\\_set.py \(3107\)](#)

## **11.158 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`.*

### 11.158.1 Detailed Description

IPv6 ROA prefix.

Definition at line 756 of file resource\_set.py.

### 11.158.2 Member Data Documentation

#### 11.158.2.1 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:

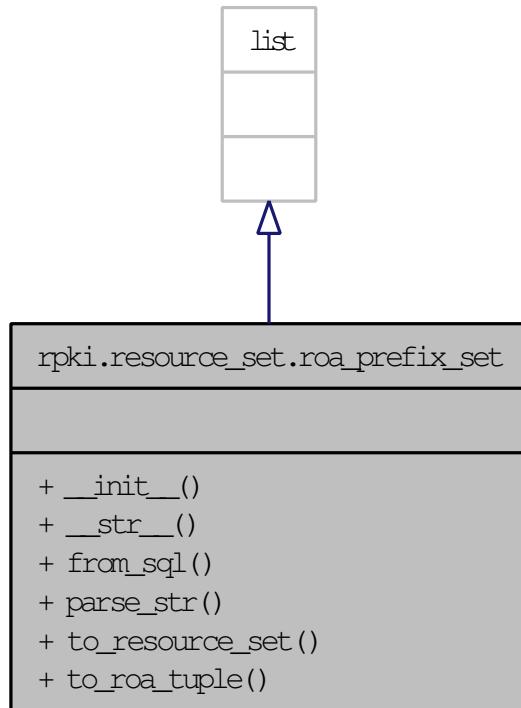
- [resource\\_set.py \(3107\)](#)

## 11.159 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](#)

#### 11.159.1 Detailed Description

Set of ROA prefixes, analogous to the `resource_set_ip` class.

Definition at line 766 of file `resource_set.py`.

## 11.159.2 Member Function Documentation

### 11.159.2.1 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.

### 11.159.2.2 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.

### 11.159.2.3 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.

### 11.159.2.4 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.

### 11.159.2.5 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`.

#### **11.159.2.6 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`.

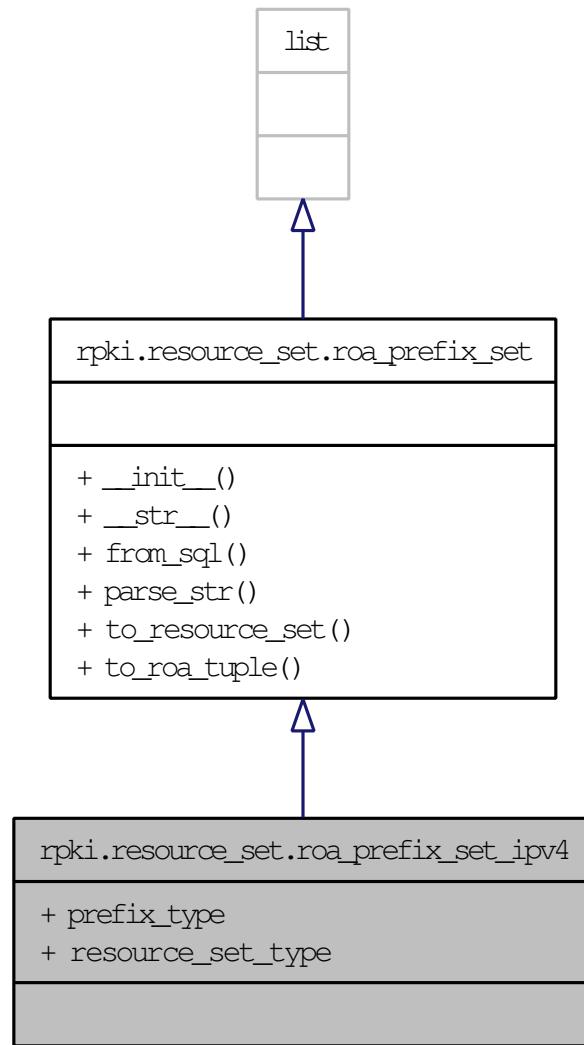
The documentation for this class was generated from the following file:

- [resource\\_set.py \(3107\)](#)

## **11.160 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.*

### 11.160.1 Detailed Description

Set of IPv4 ROA prefixes.

Definition at line 850 of file resource\_set.py.

### 11.160.2 Member Data Documentation

**11.160.2.1 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.

**11.160.2.2 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.

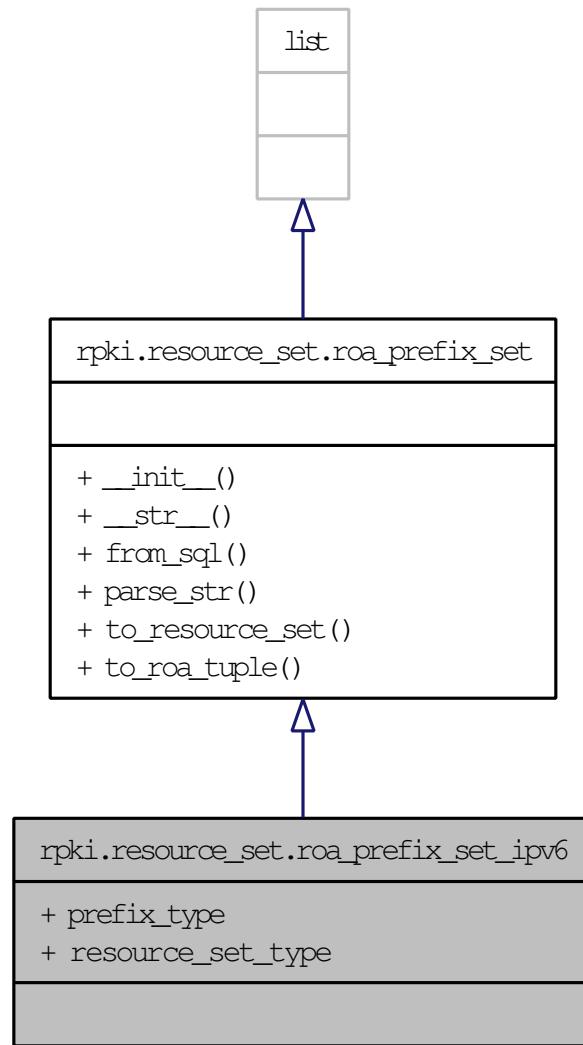
The documentation for this class was generated from the following file:

- [resource\\_set.py \(3107\)](#)

## 11.161 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.*

### 11.161.1 Detailed Description

Set of IPv6 ROA prefixes.

Definition at line 865 of file resource\_set.py.

### 11.161.2 Member Data Documentation

**11.161.2.1 `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.

**11.161.2.2 `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.

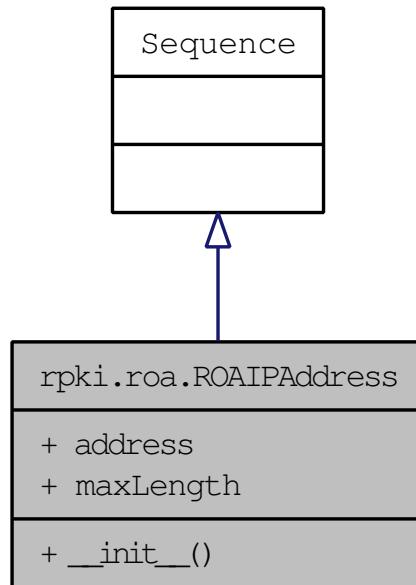
The documentation for this class was generated from the following file:

- [resource\\_set.py \(3107\)](#)

## 11.162 rpki.roa.ROAIPAddress Class Reference

Inherits [Sequence](#).

Collaboration diagram for rpki.roa.ROAIPAddress:



### Public Member Functions

- def [\\_\\_init\\_\\_](#)

### Public Attributes

- [address](#)
- [maxLength](#)

#### 11.162.1 Detailed Description

Definition at line 47 of file roa.py.

#### 11.162.2 Member Function Documentation

##### 11.162.2.1 def rpki.roa.ROAIPAddress.\_\_init\_\_(self, optional=0, default="")

Definition at line 48 of file roa.py.

### 11.162.3 Member Data Documentation

#### 11.162.3.1 rpki.roa.ROAIPAddress.address

Definition at line 49 of file roa.py.

#### 11.162.3.2 rpki.roa.ROAIPAddress.maxLength

Definition at line 50 of file roa.py.

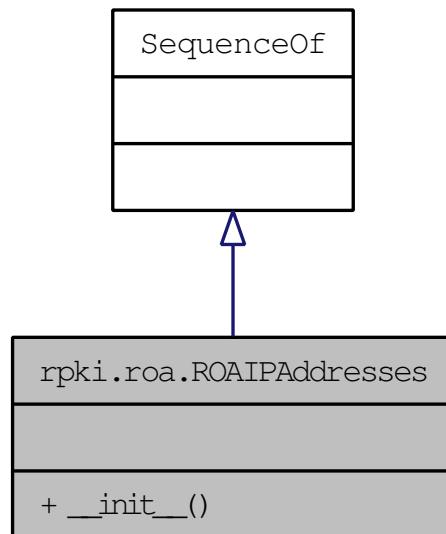
The documentation for this class was generated from the following file:

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

## 11.163 rpki.roa.ROAIPAddresses Class Reference

Inherits [SequenceOf](#).

Collaboration diagram for rpki.roa.ROAIPAddresses:



### Public Member Functions

- def [\\_\\_init\\_\\_](#)

#### 11.163.1 Detailed Description

Definition at line 54 of file roa.py.

#### 11.163.2 Member Function Documentation

##### 11.163.2.1 def rpkি.roa.ROAIPAddresses.\_\_init\_\_ (*self*, *optional* = 0, *default* = '')

Definition at line 55 of file roa.py.

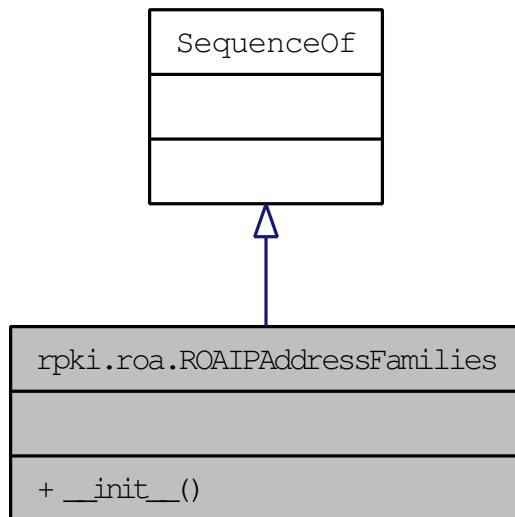
The documentation for this class was generated from the following file:

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

## 11.164 rpkি.roa.ROAIPAddressFamilies Class Reference

Inherits [SequenceOf](#).

Collaboration diagram for rpkি.roa.ROAIPAddressFamilies:



## Public Member Functions

- def [\\_\\_init\\_\\_](#)

### 11.164.1 Detailed Description

Definition at line 65 of file roa.py.

### 11.164.2 Member Function Documentation

#### 11.164.2.1 def rpki.roa.ROAIPAddressFamilies.\_\_init\_\_ (*self*, *optional* = 0, *default* = "")

Definition at line 66 of file roa.py.

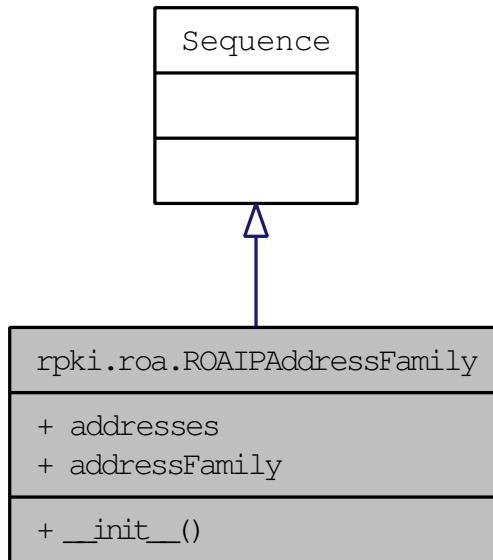
The documentation for this class was generated from the following file:

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

## 11.165 rpki.roa.ROAIPAddressFamily Class Reference

Inherits [Sequence](#).

Collaboration diagram for rpki.roa.ROAIPAddressFamily:



## Public Member Functions

- def [\\_\\_init\\_\\_](#)

## Public Attributes

- [addresses](#)
- [addressFamily](#)

### 11.165.1 Detailed Description

Definition at line 58 of file roa.py.

### 11.165.2 Member Function Documentation

#### 11.165.2.1 def rpki.roa.ROAIPAddressFamily.\_\_init\_\_ (*self*, *optional* = 0, *default* = "")

Definition at line 59 of file roa.py.

### 11.165.3 Member Data Documentation

#### 11.165.3.1 rpki.roa.ROAIPAddressFamily.addresses

Definition at line 61 of file roa.py.

#### 11.165.3.2 rpki.roa.ROAIPAddressFamily.addressFamily

Definition at line 60 of file roa.py.

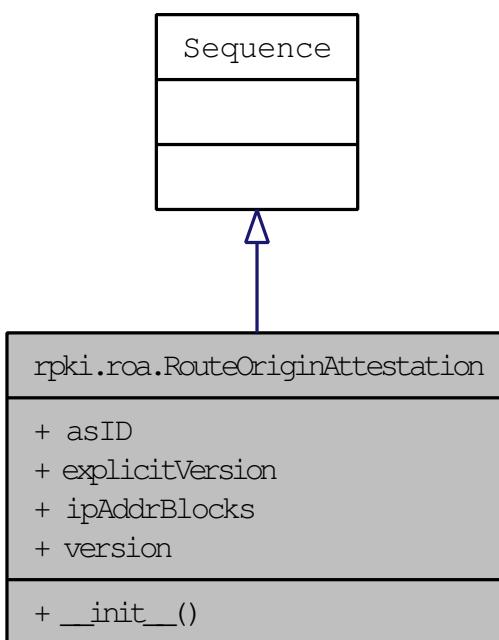
The documentation for this class was generated from the following file:

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

## 11.166 rpki.roa.RouteOriginAttestation Class Reference

Inherits [Sequence](#).

Collaboration diagram for rpki.roa.RouteOriginAttestation:



### Public Member Functions

- def [\\_\\_init\\_\\_](#)

### Public Attributes

- [asID](#)
- [explicitVersion](#)
- [ipAddrBlocks](#)
- [version](#)

#### 11.166.1 Detailed Description

Definition at line 69 of file roa.py.

#### 11.166.2 Member Function Documentation

##### 11.166.2.1 def rpkি.roa.RouteOriginAttestation.\_\_init\_\_ (*self*, *optional* = 0, *default* = '')

Definition at line 70 of file roa.py.

#### 11.166.3 Member Data Documentation

##### 11.166.3.1 rpkি.roa.RouteOriginAttestation.asID

Definition at line 73 of file roa.py.

##### 11.166.3.2 rpkি.roa.RouteOriginAttestation.explicitVersion

Definition at line 72 of file roa.py.

##### 11.166.3.3 rpkি.roa.RouteOriginAttestation.ipAddrBlocks

Definition at line 74 of file roa.py.

**11.166.3.4 rpki.roa.RouteOriginAttestation.version**

Definition at line 71 of file roa.py.

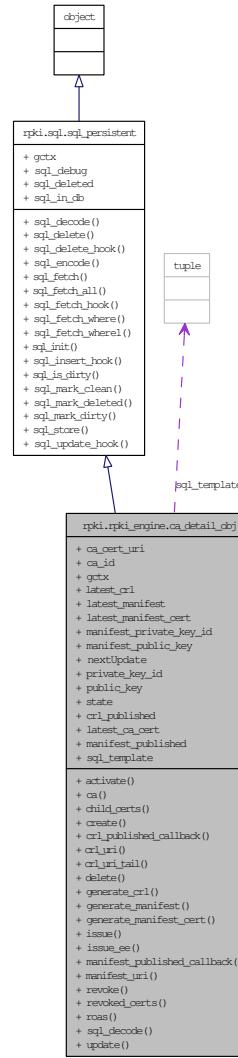
The documentation for this class was generated from the following file:

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

**11.167 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`

#### 11.167.1 Detailed Description

Internal CA detail object.

Definition at line 562 of file rpki\_engine.py.

### 11.167.2 Member Function Documentation

**11.167.2.1 def rpkি.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.

**11.167.2.2 def rpkি.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.

**11.167.2.3 def rpkি.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.

**11.167.2.4 def rpkি.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.

**11.167.2.5 def rpkি.rpki\_engine.ca\_detail\_obj.crl\_published\_callback ( *self*, *pdu*)**

Check result of CRL publication.

Definition at line 885 of file rpki\_engine.py.

**11.167.2.6 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.

**11.167.2.7 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.

**11.167.2.8 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.

**11.167.2.9 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.

**11.167.2.10 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.

**11.167.2.11 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.

**11.167.2.12 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.

**11.167.2.13 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.

**11.167.2.14 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.

**11.167.2.15 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.

**11.167.2.16 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.

**11.167.2.17 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.

**11.167.2.18 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.

**11.167.2.19 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.

**11.167.2.20 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.

**11.167.3 Member Data Documentation****11.167.3.1 rpki.rpki\_engine.ca\_detail\_obj.ca\_cert\_uri**

Definition at line 632 of file rpki\_engine.py.

**11.167.3.2 rpki.rpki\_engine.ca\_detail\_obj.ca\_id**

Definition at line 768 of file rpki\_engine.py.

**11.167.3.3 rpki.rpki\_engine.ca\_detail\_obj.crl\_published = None [static]**

Definition at line 584 of file rpki\_engine.py.

**11.167.3.4 rpki.rpki\_engine.ca\_detail\_obj.gctx**

Reimplemented from [rpki.sql.sql\\_persistent](#).

Definition at line 767 of file rpki\_engine.py.

**11.167.3.5 rpki.rpki\_engine.ca\_detail\_obj.latest\_ca\_cert = None [static]**

Definition at line 586 of file rpki\_engine.py.

**11.167.3.6 rpki.rpki\_engine.ca\_detail\_obj.latest\_crl**

Definition at line 872 of file rpki\_engine.py.

**11.167.3.7 rpki.rpki\_engine.ca\_detail\_obj.latest\_manifest**

Definition at line 913 of file rpki\_engine.py.

**11.167.3.8 rpki.rpki\_engine.ca\_detail\_obj.latest\_manifest\_cert**

Definition at line 730 of file rpki\_engine.py.

**11.167.3.9 rpki.rpki\_engine.ca\_detail\_obj.manifest\_private\_key\_id**

Definition at line 728 of file rpki\_engine.py.

**11.167.3.10 rpki.rpki\_engine.ca\_detail\_obj.manifest\_public\_key**

Definition at line 729 of file rpki\_engine.py.

**11.167.3.11 rpki.rpki\_engine.ca\_detail\_obj.manifest\_published = None  
[static]**

Definition at line 585 of file rpki\_engine.py.

**11.167.3.12 rpki.rpki\_engine.ca\_detail\_obj.nextUpdate**

Definition at line 706 of file rpki\_engine.py.

**11.167.3.13 rpki.rpki\_engine.ca\_detail\_obj.private\_key\_id**

Definition at line 727 of file rpki\_engine.py.

**11.167.3.14 rpki.rpki\_engine.ca\_detail\_obj.public\_key**

Definition at line 772 of file rpki\_engine.py.

**11.167.3.15 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.

**11.167.3.16 rpki.rpki\_engine.ca\_detail\_obj.state**

Definition at line 634 of file rpki\_engine.py.

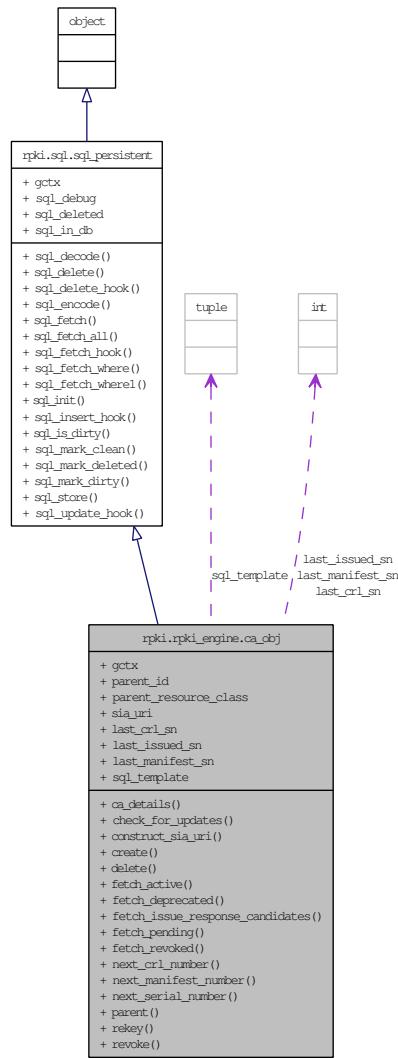
The documentation for this class was generated from the following file:

- [rpki\\_engine.py \(3107\)](#)

**11.168 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`

### 11.168.1 Detailed Description

Internal CA object.

Definition at line 308 of file rpki\_engine.py.

### 11.168.2 Member Function Documentation

#### 11.168.2.1 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.

**11.168.2.2 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.

**11.168.2.3 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.

**11.168.2.4 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.

**11.168.2.5 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.

**11.168.2.6 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.

**11.168.2.7 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.

**11.168.2.8 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.

**11.168.2.9 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.

**11.168.2.10 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.

**11.168.2.11 def rpki.rpki\_engine.ca\_obj.next\_crl\_number (*self*)**

Allocate a CRL serial number.

Definition at line 517 of file rpki\_engine.py.

**11.168.2.12 def rpki.rpki\_engine.ca\_obj.next\_manifest\_number (*self*)**

Allocate a manifest serial number.

Definition at line 509 of file rpki\_engine.py.

**11.168.2.13 def rpki.rpki\_engine.ca\_obj.next\_serial\_number (*self*)**

Allocate a certificate serial number.

Definition at line 501 of file rpki\_engine.py.

**11.168.2.14 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.

**11.168.2.15 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.

**11.168.2.16 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.

**11.168.3 Member Data Documentation****11.168.3.1 rpki.rpki\_engine.ca\_obj.gctx**

Reimplemented from [rpki.sql.sql\\_persistent](#).

Definition at line 458 of file rpki\_engine.py.

**11.168.3.2 int rpki.rpki\_engine.ca\_obj.last\_crl\_sn = 0 [static]**

Definition at line 322 of file rpki\_engine.py.

**11.168.3.3 int rpki.rpki\_engine.ca\_obj.last\_issued\_sn = 0 [static]**

Definition at line 323 of file rpki\_engine.py.

**11.168.3.4 int rpki.rpki\_engine.ca\_obj.last\_manifest\_sn = 0 [static]**

Definition at line 324 of file rpki\_engine.py.

**11.168.3.5 rpki.rpki\_engine.ca\_obj.parent\_id**

Definition at line 459 of file rpki\_engine.py.

**11.168.3.6 rpki.rpki\_engine.ca\_obj.parent\_resource\_class**

Definition at line 460 of file rpki\_engine.py.

#### 11.168.3.7 rpkirpki\_engine.ca\_obj.sia\_uri

Definition at line 382 of file rpki\_engine.py.

#### 11.168.3.8 tuple rpkirpki\_engine.ca\_obj.sql\_template [static]

**Initial value:**

```
rpkirpki.Engine.sql.template(  
    "ca",  
    "ca_id",  
    "last_crl_sn",  
    ("next_crl_update", rpkirpki.Engine.sundial.datetime),  
    "last_issued_sn", "last_manifest_sn",  
    ("next_manifest_update", rpkirpki.Engine.sundial.datetime),  
    "sia_uri", "parent_id", "parent_resource_class")
```

Definition at line 313 of file rpki\_engine.py.

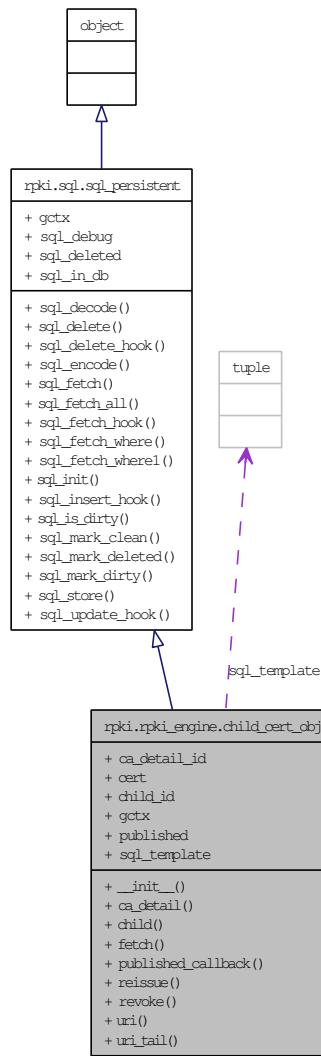
The documentation for this class was generated from the following file:

- [rpki\\_engine.py \(3107\)](#)

## 11.169 rpkirpki\_engine.child\_cert\_obj Class Reference

Inherits [rpkirpki::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](#)

#### 11.169.1 Detailed Description

Certificate that has been issued to a child.

Definition at line 936 of file rpki\_engine.py.

#### 11.169.2 Member Function Documentation

##### 11.169.2.1 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.

##### 11.169.2.2 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.

**11.169.2.3 def rpkirpki\_engine.child\_cert\_obj.child ( self)**

Fetch child object to which this child\_cert object links.

Definition at line 963 of file rpkirpki\_engine.py.

**11.169.2.4 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 rpkirpki\_engine.py.

**11.169.2.5 def rpkirpki\_engine.child\_cert\_obj.published\_callback ( self, pdu)**

Publication callback: check result and mark published.

Definition at line 1080 of file rpkirpki\_engine.py.

**11.169.2.6 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 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 rpkirpki\_engine.py.

**11.169.2.7 def rpkirpki\_engine.child\_cert\_obj.revoke ( self, publisher)**

Revoke a child cert.

Definition at line 979 of file rpkirpki\_engine.py.

**11.169.2.8 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.

**11.169.2.9 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.

**11.169.3 Member Data Documentation****11.169.3.1 rpki.rpki\_engine.child\_cert\_obj.ca\_detail\_id**

Definition at line 957 of file rpki\_engine.py.

**11.169.3.2 rpki.rpki\_engine.child\_cert\_obj.cert**

Definition at line 958 of file rpki\_engine.py.

**11.169.3.3 rpki.rpki\_engine.child\_cert\_obj.child\_id**

Definition at line 956 of file rpki\_engine.py.

**11.169.3.4 rpki.rpki\_engine.child\_cert\_obj.gctx**

Reimplemented from [rpki.sql.sql\\_persistent](#).

Definition at line 955 of file rpki\_engine.py.

**11.169.3.5 rpki.rpki\_engine.child\_cert\_obj.published**

Definition at line 959 of file rpki\_engine.py.

**11.169.3.6 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.

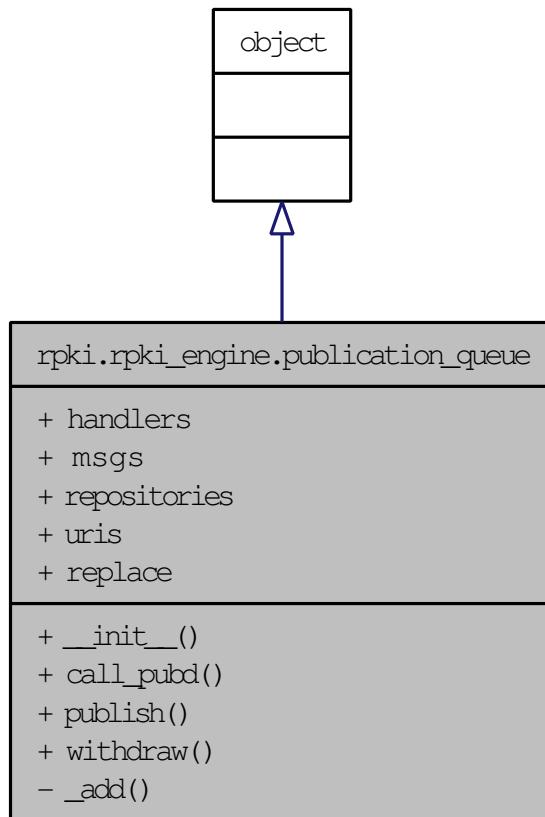
The documentation for this class was generated from the following file:

- [rpki\\_engine.py \(3107\)](#)

**11.170 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`

**11.170.1 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.

**11.170.2 Member Function Documentation****11.170.2.1 def rpkid.rpki\_engine.publication\_queue.\_\_init\_\_ (*self*)**

Definition at line 1379 of file rpki\_engine.py.

**11.170.2.2 def rpkid.rpki\_engine.publication\_queue.\_add (*self, cls, uri, obj, repository, handler, withdraw*) [private]**

Definition at line 1386 of file rpki\_engine.py.

**11.170.2.3 def rpkid.rpki\_engine.publication\_queue.call\_pubd (*self, cb, eb*)**

Definition at line 1409 of file rpki\_engine.py.

**11.170.2.4 def rpkid.rpki\_engine.publication\_queue.publish (*self, cls, uri, obj, repository, handler = None*)**

Definition at line 1403 of file rpki\_engine.py.

#### 11.170.2.5 def rpki.rpki\_engine.publication\_queue.withdraw (*self*, *cls*, *uri*, *obj*, *repository*, *handler* = **None**)

Definition at line 1406 of file rpki\_engine.py.

### 11.170.3 Member Data Documentation

#### 11.170.3.1 rpki.rpki\_engine.publication\_queue.handlers

Definition at line 1382 of file rpki\_engine.py.

#### 11.170.3.2 rpki.rpki\_engine.publication\_queue.msgs

Definition at line 1381 of file rpki\_engine.py.

#### 11.170.3.3 rpki.rpki\_engine.publication\_queue.replace = True [static]

Definition at line 1377 of file rpki\_engine.py.

#### 11.170.3.4 rpki.rpki\_engine.publication\_queue.repositories

Definition at line 1380 of file rpki\_engine.py.

#### 11.170.3.5 rpki.rpki\_engine.publication\_queue.uris

Definition at line 1384 of file rpki\_engine.py.

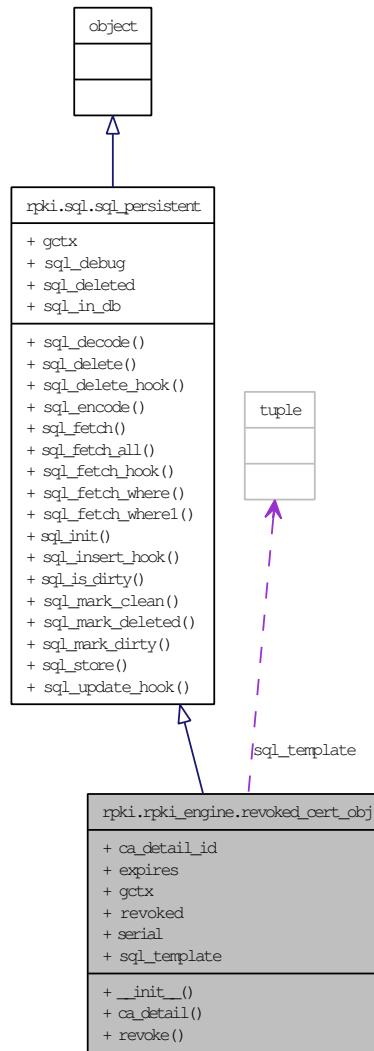
The documentation for this class was generated from the following file:

- [rpki\\_engine.py \(3107\)](#)

## 11.171 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](#)

#### 11.171.1 Detailed Description

Tombstone for a revoked certificate.

Definition at line 1088 of file rpki\_engine.py.

#### 11.171.2 Member Function Documentation

##### 11.171.2.1 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.

##### 11.171.2.2 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.

**11.171.2.3 def rpki.rpki\_engine.revoked\_cert\_obj.revoke (*cls, cert, ca\_detail*)**

Revoke a certificate.

Definition at line 1117 of file rpki\_engine.py.

**11.171.3 Member Data Documentation****11.171.3.1 rpki.rpki\_engine.revoked\_cert\_obj.ca\_detail\_id**

Definition at line 1108 of file rpki\_engine.py.

**11.171.3.2 rpki.rpki\_engine.revoked\_cert\_obj.expires**

Definition at line 1107 of file rpki\_engine.py.

**11.171.3.3 rpki.rpki\_engine.revoked\_cert\_obj.gctx**

Reimplemented from [rpki.sql.sql\\_persistent](#).

Definition at line 1104 of file rpki\_engine.py.

**11.171.3.4 rpki.rpki\_engine.revoked\_cert\_obj.revoked**

Definition at line 1106 of file rpki\_engine.py.

**11.171.3.5 rpki.rpki\_engine.revoked\_cert\_obj.serial**

Definition at line 1105 of file rpki\_engine.py.

**11.171.3.6 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.

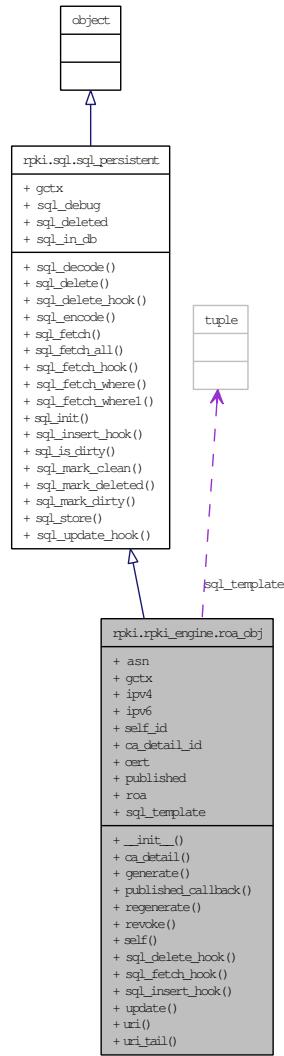
The documentation for this class was generated from the following file:

- [rpki\\_engine.py \(3107\)](#)

## 11.172 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](#)

#### 11.172.1 Detailed Description

Route Origin Authorization.

Definition at line 1128 of file rpkirpki\_engine.py.

#### 11.172.2 Member Function Documentation

##### 11.172.2.1 def rpkirpki\_engine.roa\_obj.\_\_init\_\_ ( self, gctx = None, self\_id = None, asn = None, ipv4 = None, ipv6 = None )

Definition at line 1194 of file rpkirpki\_engine.py.

**11.172.2.2 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.

**11.172.2.3 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.

**11.172.2.4 def rpkি.rpki\_engine.roa\_obj.published\_callback (*self, pdu*)**

Check publication result.

Definition at line 1303 of file rpki\_engine.py.

**11.172.2.5 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.

**11.172.2.6 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.

**11.172.2.7 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.

**11.172.2.8 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.

**11.172.2.9 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.

**11.172.2.10 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.

### 11.172.2.11 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.

### 11.172.2.12 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.

### 11.172.2.13 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.

## 11.172.3 Member Data Documentation

### 11.172.3.1 rpki.rpki\_engine.roa\_obj.asn

Definition at line 1198 of file rpki\_engine.py.

### 11.172.3.2 rpki.rpki\_engine.roa\_obj.ca\_detail\_id = None [static]

Definition at line 1143 of file rpki\_engine.py.

**11.172.3.3 rpki.rpki\_engine.roa\_obj.cert = None [static]**

Definition at line 1144 of file rpki\_engine.py.

**11.172.3.4 rpki.rpki\_engine.roa\_obj.gctx**

Reimplemented from [rpki.sql.sql\\_persistent](#).

Definition at line 1196 of file rpki\_engine.py.

**11.172.3.5 rpki.rpki\_engine.roa\_obj.ipv4**

Definition at line 1199 of file rpki\_engine.py.

**11.172.3.6 rpki.rpki\_engine.roa\_obj.ipv6**

Definition at line 1200 of file rpki\_engine.py.

**11.172.3.7 rpki.rpki\_engine.roa\_obj.published = None [static]**

Definition at line 1146 of file rpki\_engine.py.

**11.172.3.8 rpki.rpki\_engine.roa\_obj.roa = None [static]**

Definition at line 1145 of file rpki\_engine.py.

**11.172.3.9 rpki.rpki\_engine.roa\_obj.self\_id**

Definition at line 1197 of file rpki\_engine.py.

**11.172.3.10 tuple rpki.rpki\_engine.roa\_obj.sql\_template [static]**

**Initial value:**

```
rpkisqltemplate(
    "roa",
    "roa_id",
    "ca_detail_id",
    "self_id",
    "asn",
    ("roa", rpkix509.ROA),
    ("cert", rpkix509.X509),
    ("published", rpkisundial.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)

## 11.173 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)

#### 11.173.1 Detailed Description

A container for various global rpkid parameters.

Definition at line 39 of file rpkid\_engine.py.

### 11.173.2 Member Function Documentation

#### 11.173.2.1 def rpkid\_context.\_\_init\_\_ (*self*, *cfg*)

Definition at line 44 of file rpkid\_context.py.

#### 11.173.2.2 def rpkid\_context.build\_https\_ta\_cache (*self*)

Build dynamic TLS trust anchors.

Definition at line 288 of file rpkid\_context.py.

#### 11.173.2.3 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.

#### 11.173.2.4 def rpkid\_context.clear\_https\_ta\_cache (*self*)

Clear dynamic TLS trust anchors.

Definition at line 279 of file rpkid\_context.py.

#### 11.173.2.5 def rpkid\_context.cron (*self*, *cb* = **None**)

Periodic tasks.

Definition at line 207 of file rpkid\_context.py.

**11.173.2.6 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.

**11.173.2.7 def rpkid\_context.irdb\_query (self, q\_pdu, callback, errback)**

Perform an IRDB callback query.

Definition at line 86 of file rpkid\_context.py.

**11.173.2.8 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.

**11.173.2.9 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.

**11.173.2.10 def rpkid\_context.left\_right\_handler (self, query, path, cb)**

Process one left-right PDU.

Definition at line 146 of file rpkid\_context.py.

**11.173.2.11 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.

**11.173.2.12 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.

**11.173.3 Member Data Documentation****11.173.3.1 rpki.rpki\_engine.rpkid\_context.bpk1\_ta**

Definition at line 48 of file rpki\_engine.py.

**11.173.3.2 rpki.rpki\_engine.rpkid\_context.cron\_keepalive**

Definition at line 68 of file rpki\_engine.py.

**11.173.3.3 rpki.rpki\_engine.rpkid\_context.cron\_period**

Definition at line 67 of file rpki\_engine.py.

**11.173.3.4 rpki.rpki\_engine.rpkid\_context.cron\_timeout**

Definition at line 71 of file rpki\_engine.py.

**11.173.3.5 rpki.rpki\_engine.rpkid\_context.cron\_timer**

Definition at line 79 of file rpki\_engine.py.

**11.173.3.6 rpki.rpki\_engine.rpkid\_context.https\_server\_host**

Definition at line 56 of file rpki\_engine.py.

**11.173.3.7 rpki.rpki\_engine.rpkid\_context.https\_server\_port**

Definition at line 57 of file rpki\_engine.py.

**11.173.3.8 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.

**11.173.3.9 rpki.rpki\_engine.rpkid\_context.initial\_delay**

Definition at line 63 of file rpki\_engine.py.

**11.173.3.10 rpki.rpki\_engine.rpkid\_context.irbe\_cert**

Definition at line 50 of file rpki\_engine.py.

**11.173.3.11 rpki.rpki\_engine.rpkid\_context.irdb\_cert**

Definition at line 49 of file rpki\_engine.py.

**11.173.3.12 rpki.rpki\_engine.rpkid\_context.irdb\_url**

Definition at line 54 of file rpki\_engine.py.

**11.173.3.13 rpki.rpki\_engine.rpkid\_context.publication\_kludge\_base**

Definition at line 59 of file rpki\_engine.py.

**11.173.3.14 rpki.rpki\_engine.rpkid\_context.rpkid\_cert**

Definition at line 51 of file rpki\_engine.py.

**11.173.3.15 rpki.rpki\_engine.rpkid\_context.rpkid\_key**

Definition at line 52 of file rpki\_engine.py.

**11.173.3.16 rpki.rpki\_engine.rpkid\_context.sql**

Definition at line 46 of file rpki\_engine.py.

**11.173.3.17 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.

**11.173.3.18 rpki.rpki\_engine.rpkid\_context.use\_internal\_cron**

Definition at line 61 of file rpki\_engine.py.

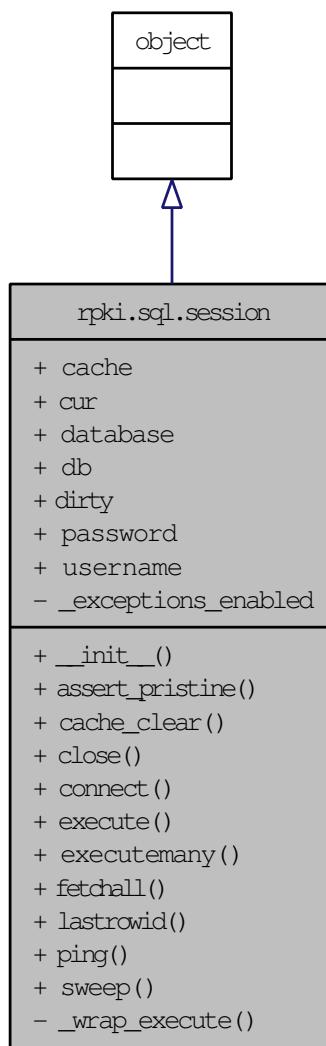
The documentation for this class was generated from the following file:

- [rpkি\\_engine.py \(3107\)](#)

## 11.174 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

#### 11.174.1 Detailed Description

SQL session layer.

Definition at line 50 of file sql.py.

### 11.174.2 Member Function Documentation

#### 11.174.2.1 def rpkি.sql.session.\_\_init\_\_ (*self*, *cfg*)

Definition at line 57 of file sql.py.

#### 11.174.2.2 def rpkি.sql.session.\_wrap\_execute (*self*, *func*, *query*, *args*) [private]

Definition at line 88 of file sql.py.

#### 11.174.2.3 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.

#### 11.174.2.4 def rpkি.sql.session.cache\_clear (*self*)

Clear the object cache.

Definition at line 108 of file sql.py.

#### 11.174.2.5 def rpkি.sql.session.close (*self*)

Definition at line 77 of file sql.py.

#### 11.174.2.6 def rpkি.sql.session.connect (*self*)

Definition at line 72 of file sql.py.

**11.174.2.7 def rpki.sql.session.execute ( *self*, *query*, *args* = **None**)**

Definition at line 96 of file sql.py.

**11.174.2.8 def rpki.sql.session.executemany ( *self*, *query*, *args*)**

Definition at line 99 of file sql.py.

**11.174.2.9 def rpki.sql.session.fetchall ( *self*)**

Definition at line 102 of file sql.py.

**11.174.2.10 def rpki.sql.session.lastrowid ( *self*)**

Definition at line 105 of file sql.py.

**11.174.2.11 def rpki.sql.session.ping ( *self*)**

Definition at line 85 of file sql.py.

**11.174.2.12 def rpki.sql.session.sweep ( *self*)**

Write any dirty objects out to SQL.

Definition at line 116 of file sql.py.

**11.174.3 Member Data Documentation****11.174.3.1 rpki.sql.session.\_exceptions\_enabled = False [static, private]**

Definition at line 55 of file sql.py.

**11.174.3.2 rpki.sql.session.cache**

Definition at line 67 of file sql.py.

**11.174.3.3 rpki.sql.session.cur**

Definition at line 74 of file sql.py.

**11.174.3.4 rpki.sql.session.database**

Definition at line 64 of file sql.py.

**11.174.3.5 rpki.sql.session.db**

Definition at line 73 of file sql.py.

**11.174.3.6 rpki.sql.session.dirty**

Definition at line 68 of file sql.py.

**11.174.3.7 rpki.sql.session.password**

Definition at line 65 of file sql.py.

**11.174.3.8 rpki.sql.session.username**

Definition at line 63 of file sql.py.

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

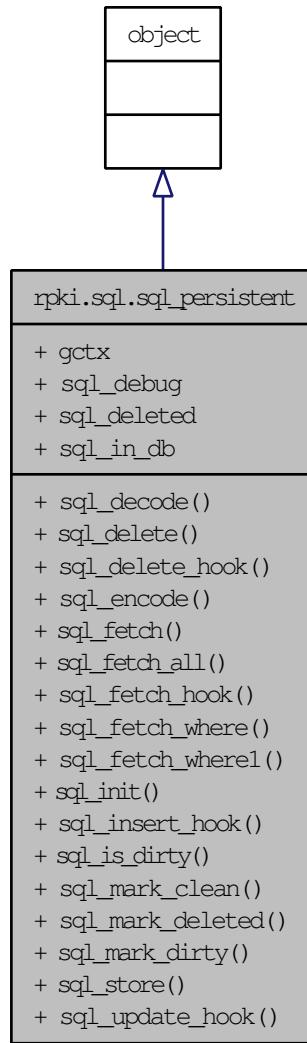
- [sql.py \(2895\)](#)

## 11.175 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 rpki.sql.sql\_persistent:



### Public Member Functions

- def [sql\\_decode](#)
- def [sql\\_delete](#)
- def [sql\\_delete\\_hook](#)
- def [sql\\_encode](#)
- def [sql\\_fetch](#)

- def [sql\\_fetch\\_all](#)
- def [sql\\_fetch\\_hook](#)
- def [sql\\_fetch\\_where](#)
- def [sql\\_fetch\\_where1](#)
- def [sql\\_init](#)
- def [sql\\_insert\\_hook](#)
- def [sql\\_is\\_dirty](#)
- def [sql\\_mark\\_clean](#)
- def [sql\\_mark\\_deleted](#)
- def [sql\\_mark\\_dirty](#)
- def [sql\\_store](#)
- def [sql\\_update\\_hook](#)

### Public Attributes

- [gctx](#)

### Static Public Attributes

- [sql\\_debug](#) = False  
*Enable logging of SQL actions.*
- [sql\\_deleted](#) = False  
*Whether our cached copy of this object has been deleted.*
- [sql\\_in\\_db](#) = False  
*Whether this object is already in SQL or not.*

### 11.175.1 Detailed Description

Mixin for persistent class that needs to be stored in SQL.

Definition at line 152 of file `sql.py`.

### 11.175.2 Member Function Documentation

#### 11.175.2.1 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.

#### 11.175.2.2 def rpkি.sql.sql\_persistent.sql\_delete (*self*)

Delete this object from SQL.

Definition at line 293 of file sql.py.

#### 11.175.2.3 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.

#### 11.175.2.4 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.

#### 11.175.2.5 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.

#### 11.175.2.6 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.

#### 11.175.2.7 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.

#### 11.175.2.8 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.

#### 11.175.2.9 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.

**11.175.2.10 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.

**11.175.2.11 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.

**11.175.2.12 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.

**11.175.2.13 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.

**11.175.2.14 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.

**11.175.2.15 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.

**11.175.2.16 def rpki.sql.sql\_persistent.sql\_store ( *self* )**

Store this object to SQL.

Definition at line 271 of file sql.py.

**11.175.2.17 def rpki.sql.sql\_persistent.sql\_update\_hook ( *self* )**

Customization hook.

Definition at line 343 of file sql.py.

**11.175.3 Member Data Documentation****11.175.3.1 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.

**11.175.3.2 rpki::sql.sql\_persistent::sql\_debug = False [static]**

Enable logging of SQL actions.

Definition at line 170 of file sql.py.

**11.175.3.3 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.

**11.175.3.4 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.

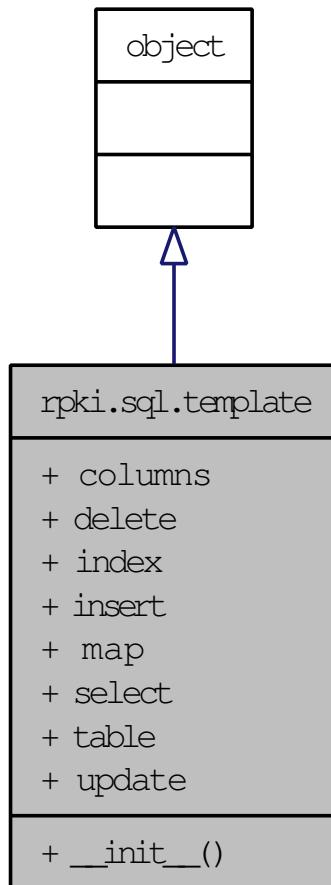
The documentation for this class was generated from the following file:

- [sql.py \(2895\)](#)

**11.176 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](#)

### 11.176.1 Detailed Description

SQL template generator.

Definition at line 128 of file sql.py.

### 11.176.2 Member Function Documentation

#### 11.176.2.1 def rpkি.sql.template.\_\_init\_\_ ( *self*, *table\_name*, *index\_column*, *data\_columns* )

Build a SQL template.

Definition at line 133 of file sql.py.

### 11.176.3 Member Data Documentation

#### 11.176.3.1 rpkি.sql.template.columns

Definition at line 140 of file sql.py.

#### 11.176.3.2 rpkি.sql.template.delete

Definition at line 150 of file sql.py.

#### 11.176.3.3 rpkি.sql.template.index

Definition at line 139 of file sql.py.

**11.176.3.4 rpki.sql.template.insert**

Definition at line 143 of file sql.py.

**11.176.3.5 rpki.sql.template.map**

Definition at line 141 of file sql.py.

**11.176.3.6 rpki.sql.template.select**

Definition at line 142 of file sql.py.

**11.176.3.7 rpki.sql.template.table**

Definition at line 138 of file sql.py.

**11.176.3.8 rpki.sql.template.update**

Definition at line 146 of file sql.py.

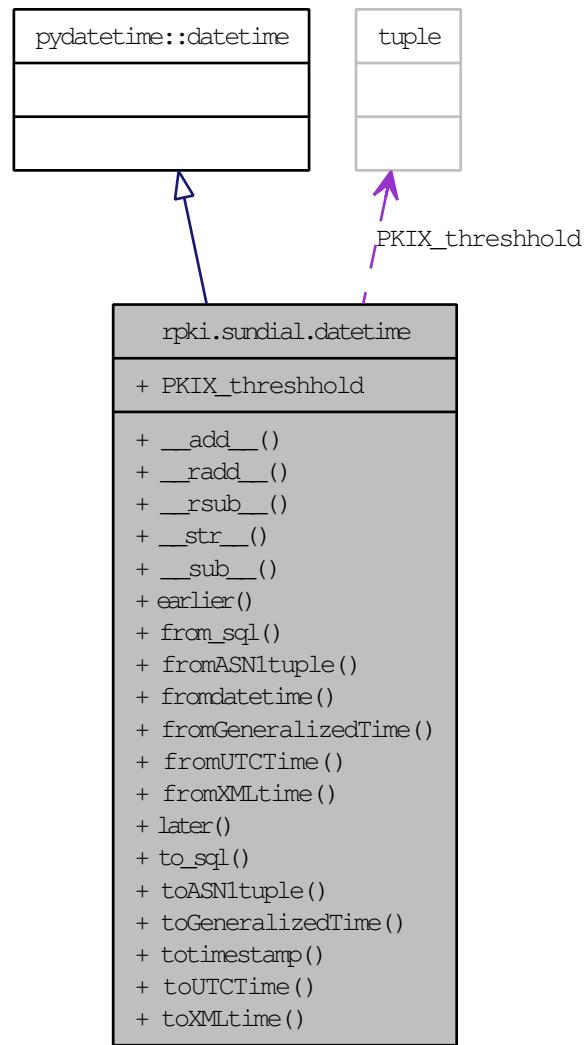
The documentation for this class was generated from the following file:

- [sql.py \(2895\)](#)

**11.177 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.*

### 11.177.1 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`.

### 11.177.2 Member Function Documentation

#### 11.177.2.1 def rpkisundial.datetime.\_\_add\_\_ (*self*, *y*)

Definition at line 163 of file `sundial.py`.

#### 11.177.2.2 def rpkisundial.datetime.\_\_radd\_\_ (*self*, *y*)

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

**11.177.2.3 def rpki.sundial.datetime.\_\_rsub\_\_ (*self*, *y*)**

Definition at line 165 of file sundial.py.

**11.177.2.4 def rpki.sundial.datetime.\_\_str\_\_ (*self*)**

Definition at line 124 of file sundial.py.

**11.177.2.5 def rpki.sundial.datetime.\_\_sub\_\_ (*self*, *y*)**

Definition at line 166 of file sundial.py.

**11.177.2.6 def rpki.sundial.datetime.earlier (*self*, *other*)**

Return the earlier of two timestamps.

Definition at line 159 of file sundial.py.

**11.177.2.7 def rpki.sundial.datetime.from\_sql (*cls*, *x*)**

Convert from SQL storage format.

Definition at line 136 of file sundial.py.

**11.177.2.8 def rpki.sundial.datetime.fromASN1tuple (*cls*, *x*)**

Convert from ASN.1 tuple representation.

Definition at line 86 of file sundial.py.

**11.177.2.9 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`.

**11.177.2.10 def rpkisundial.datetime.fromGeneralizedTime ( *cls*, *x* )**

Convert from ASN.1 GeneralizedTime.

Definition at line 77 of file `sundial.py`.

**11.177.2.11 def rpkisundial.datetime.fromUTCTime ( *cls*, *x* )**

Convert from ASN.1 UTCTime.

Definition at line 68 of file `sundial.py`.

**11.177.2.12 def rpkisundial.datetime.fromXMLtime ( *cls*, *x* )**

Convert from XML time representation.

Definition at line 111 of file `sundial.py`.

**11.177.2.13 def rpkisundial.datetime.later ( *self*, *other* )**

Return the later of two timestamps.

Definition at line 155 of file `sundial.py`.

**11.177.2.14 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.

**11.177.2.15 def rpki.sundial.datetime.toASN1tuple ( *self* )**

Convert to ASN.1 tuple representation.

Definition at line 101 of file sundial.py.

**11.177.2.16 def rpki.sundial.datetime.toGeneralizedTime ( *self* )**

Convert to ASN.1 GeneralizedTime.

Definition at line 81 of file sundial.py.

**11.177.2.17 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.

**11.177.2.18 def rpki.sundial.datetime.toUTCTime ( *self* )**

Convert to ASN.1 UTCTime.

Definition at line 72 of file sundial.py.

**11.177.2.19 def rpki.sundial.datetime.toXMLtime ( *self* )**

Convert to XML time representation.

Definition at line 120 of file sundial.py.

**11.177.3 Member Data Documentation****11.177.3.1 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.

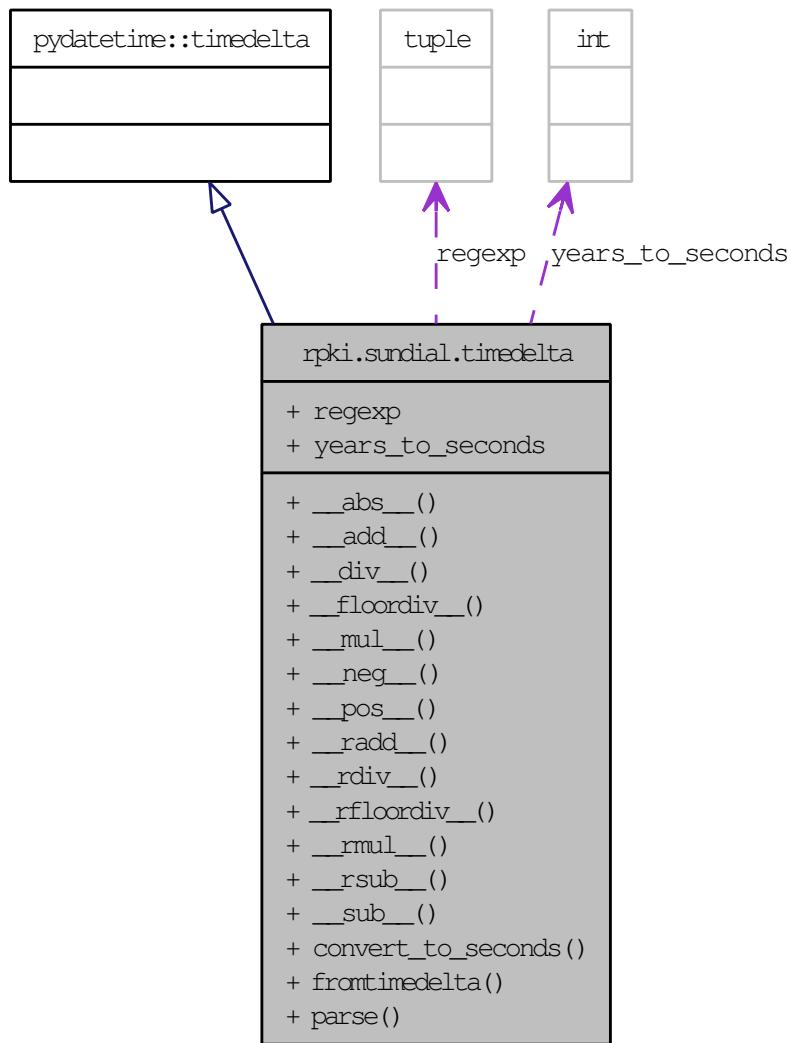
The documentation for this class was generated from the following file:

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

**11.178 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).*

### 11.178.1 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.

**11.178.2 Member Function Documentation****11.178.2.1 def rpkisundial.timedelta.\_\_abs\_\_ (*self*)**

Definition at line 243 of file sundial.py.

**11.178.2.2 def rpkisundial.timedelta.\_\_add\_\_ (*self*, *x*)**

Definition at line 244 of file sundial.py.

**11.178.2.3 def rpkisundial.timedelta.\_\_div\_\_ (*self*, *x*)**

Definition at line 245 of file sundial.py.

**11.178.2.4 def rpkisundial.timedelta.\_\_floordiv\_\_ (*self*, *x*)**

Definition at line 246 of file sundial.py.

**11.178.2.5 def rpkisundial.timedelta.\_\_mul\_\_ (*self*, *x*)**

Definition at line 247 of file sundial.py.

**11.178.2.6 def rpkisundial.timedelta.\_\_neg\_\_ (*self*)**

Definition at line 248 of file sundial.py.

**11.178.2.7 def rpkisundial.timedelta.\_\_pos\_\_ (*self*)**

Definition at line 249 of file sundial.py.

**11.178.2.8 def rpki.sundial.timedelta.\_\_radd\_\_ ( *self*, *x*)**

Definition at line 250 of file sundial.py.

**11.178.2.9 def rpki.sundial.timedelta.\_\_rdiv\_\_ ( *self*, *x*)**

Definition at line 251 of file sundial.py.

**11.178.2.10 def rpki.sundial.timedelta.\_\_rfloordiv\_\_ ( *self*, *x*)**

Definition at line 252 of file sundial.py.

**11.178.2.11 def rpki.sundial.timedelta.\_\_rmul\_\_ ( *self*, *x*)**

Definition at line 253 of file sundial.py.

**11.178.2.12 def rpki.sundial.timedelta.\_\_rsub\_\_ ( *self*, *x*)**

Definition at line 254 of file sundial.py.

**11.178.2.13 def rpki.sundial.timedelta.\_\_sub\_\_ ( *self*, *x*)**

Definition at line 255 of file sundial.py.

**11.178.2.14 def rpki.sundial.timedelta.convert\_to\_seconds ( *self*)**

Convert a timedelta interval to seconds.

Definition at line 234 of file sundial.py.

**11.178.2.15 def rpkি.sundial.timedelta.fromtimedelta ( *cls*, *x*)**

Convert a `datetime.timedelta` object into this subclass.

Definition at line 239 of file `sundial.py`.

**11.178.2.16 def rpkি.sundial.timedelta.parse ( *cls*, *arg*)**

Parse text into a `timedelta` object.

Definition at line 213 of file `sundial.py`.

**11.178.3 Member Data Documentation****11.178.3.1 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`.

**11.178.3.2 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:

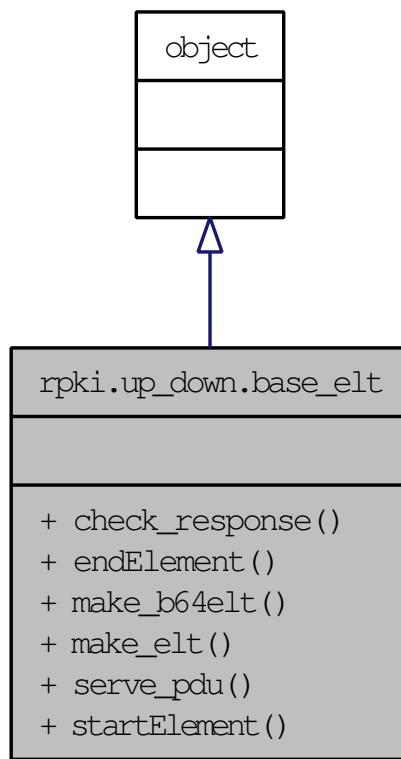
- [sundial.py \(3191\)](#)

## 11.179 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](#)

### 11.179.1 Detailed Description

Generic PDU object.

Virtual class, just provides some default methods.

Definition at line 43 of file up\_down.py.

### 11.179.2 Member Function Documentation

#### 11.179.2.1 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.

#### 11.179.2.2 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.

#### 11.179.2.3 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.

#### 11.179.2.4 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.

#### 11.179.2.5 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.

#### 11.179.2.6 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.

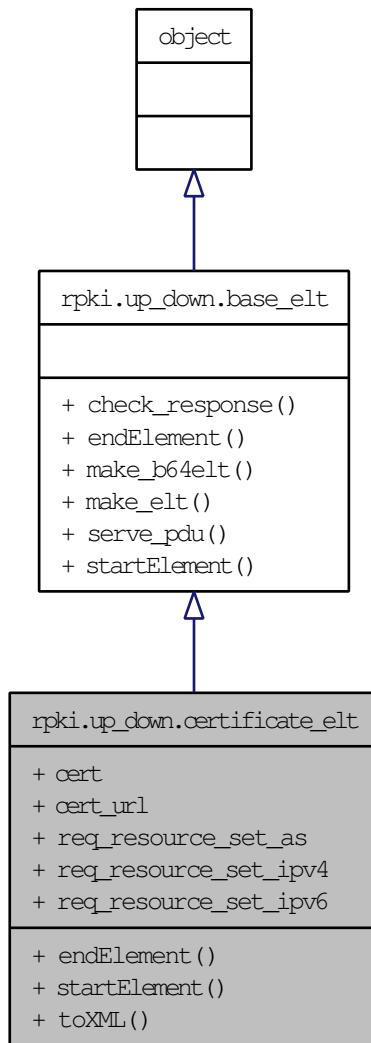
The documentation for this class was generated from the following file:

- [up\\_down.py \(3162\)](#)

## 11.180 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](#)

### 11.180.1 Detailed Description

Up-Down protocol representation of an issued certificate.

Definition at line 128 of file up\_down.py.

### 11.180.2 Member Function Documentation

#### 11.180.2.1 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.

#### 11.180.2.2 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.

#### 11.180.2.3 def rpk.up\_down.certificate\_elt.toXML (*self*)

Generate a <certificate/> element.

Definition at line 151 of file up\_down.py.

**11.180.3 Member Data Documentation****11.180.3.1 rpki.up\_down.certificate\_elt.cert**

Definition at line 148 of file up\_down.py.

**11.180.3.2 rpki.up\_down.certificate\_elt.cert\_url**

Definition at line 138 of file up\_down.py.

**11.180.3.3 rpki.up\_down.certificate\_elt.req\_resource\_set\_as**

Definition at line 139 of file up\_down.py.

**11.180.3.4 rpki.up\_down.certificate\_elt.req\_resource\_set\_ipv4**

Definition at line 140 of file up\_down.py.

**11.180.3.5 rpki.up\_down.certificate\_elt.req\_resource\_set\_ipv6**

Definition at line 141 of file up\_down.py.

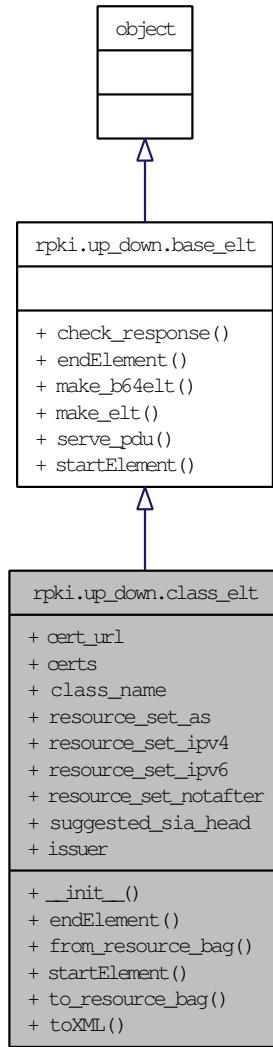
The documentation for this class was generated from the following file:

- [up\\_down.py \(3162\)](#)

**11.181 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

#### 11.181.1 Detailed Description

Up-Down protocol representation of a resource class.

Definition at line 160 of file up\_down.py.

#### 11.181.2 Member Function Documentation

##### 11.181.2.1 def rpk.up\_down.class\_elt.\_\_init\_\_ (self)

Initialize class\_elt.

Definition at line 167 of file up\_down.py.

##### 11.181.2.2 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.

**11.181.2.3 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.

**11.181.2.4 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.

**11.181.2.5 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.

**11.181.2.6 def rpki.up\_down.class\_elt.toXML (self)**

Generate a <class/> element.

Definition at line 201 of file up\_down.py.

**11.181.3 Member Data Documentation****11.181.3.1 rpki.up\_down.class\_elt.cert\_url**

Definition at line 184 of file up\_down.py.

**11.181.3.2 rpki.up\_down.class\_elt.certs**

Definition at line 170 of file up\_down.py.

**11.181.3.3 rpki.up\_down.class\_elt.class\_name**

Definition at line 183 of file up\_down.py.

**11.181.3.4 rpki.up\_down.class\_elt.issuer = None [static]**

Definition at line 165 of file up\_down.py.

**11.181.3.5 rpki.up\_down.class\_elt.resource\_set\_as**

Definition at line 186 of file up\_down.py.

**11.181.3.6 rpki.up\_down.class\_elt.resource\_set\_ipv4**

Definition at line 187 of file up\_down.py.

**11.181.3.7 rpki.up\_down.class\_elt.resource\_set\_ipv6**

Definition at line 188 of file up\_down.py.

**11.181.3.8 rpki.up\_down.class\_elt.resource\_set\_notafter**

Definition at line 189 of file up\_down.py.

**11.181.3.9 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:

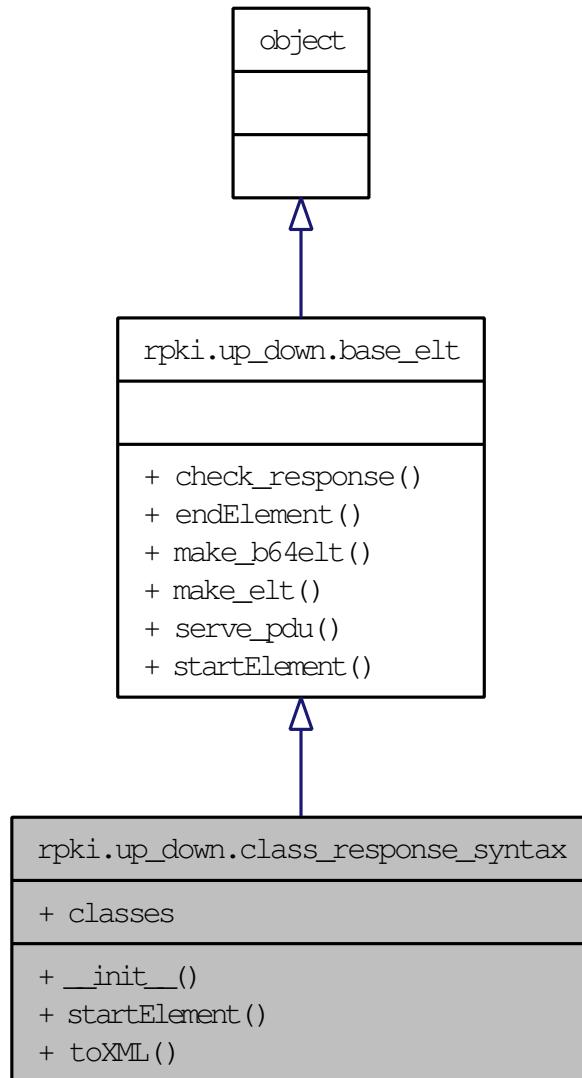
- [up\\_down.py \(3162\)](#)

## 11.182 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](#)

### 11.182.1 Detailed Description

Syntax for Up-Down protocol "list\_response" and "issue\_response" PDUs.

Definition at line 285 of file up\_down.py.

### 11.182.2 Member Function Documentation

#### 11.182.2.1 def rpk.up\_down.class\_response\_syntax.\_\_init\_\_ (*self*)

Initialize class\_response\_syntax.

Definition at line 290 of file up\_down.py.

#### 11.182.2.2 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.

#### 11.182.2.3 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.

### 11.182.3 Member Data Documentation

#### 11.182.3.1 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:

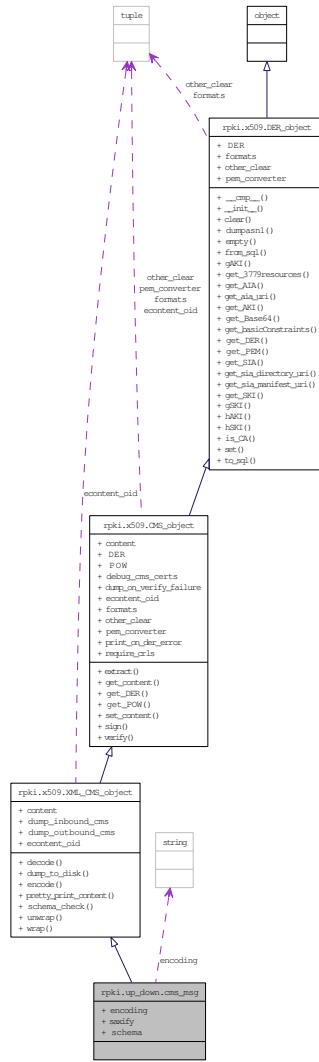
- [up\\_down.py \(3162\)](#)

## 11.183 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`

### 11.183.1 Detailed Description

Class to hold a CMS-signed up-down PDU.

Definition at line 685 of file up\_down.py.

### 11.183.2 Member Data Documentation

#### 11.183.2.1 string rpki.up\_down.cms\_msg.encoding = "UTF-8" [static]

Definition at line 690 of file up\_down.py.

#### 11.183.2.2 rpki.up\_down.cms\_msg.saxify = sax\_handler.saxify [static]

Reimplemented in [rootd.cms\\_msg](#).

Definition at line 692 of file up\_down.py.

#### 11.183.2.3 rpki.up\_down.cms\_msg.schema = rpki.relaxng.up\_down [static]

Definition at line 691 of file up\_down.py.

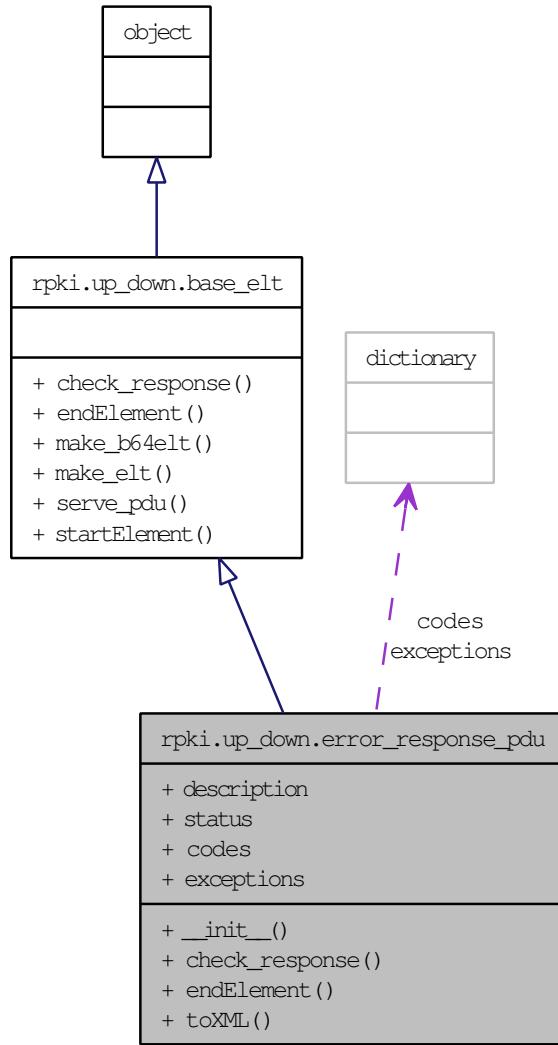
The documentation for this class was generated from the following file:

- [up\\_down.py \(3162\)](#)

## 11.184 rpki.up\_down.error\_response\_pdu Class Reference

Inherits [rpki::up\\_down::base\\_elt](#).

Collaboration diagram for rpk.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](#)

### 11.184.1 Detailed Description

Up-Down protocol "error\_response" PDU.

Definition at line 505 of file up\_down.py.

### 11.184.2 Member Function Documentation

#### 11.184.2.1 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.

#### 11.184.2.2 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.

#### 11.184.2.3 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.

#### 11.184.2.4 def rpki.up\_down.error\_response\_pdu.toXML ( *self* )

Generate payload of "error\_response" PDU.

Definition at line 549 of file up\_down.py.

### 11.184.3 Member Data Documentation

#### 11.184.3.1 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.

#### 11.184.3.2 rpki.up\_down.error\_response\_pdu.description

Definition at line 531 of file up\_down.py.

#### 11.184.3.3 dictionary rpki.up\_down.error\_response\_pdu.exceptions [static]

**Initial value:**

```
{  
    rpki.exceptions.NoActiveCA : 1202 }
```

Definition at line 521 of file up\_down.py.

**11.184.3.4 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:

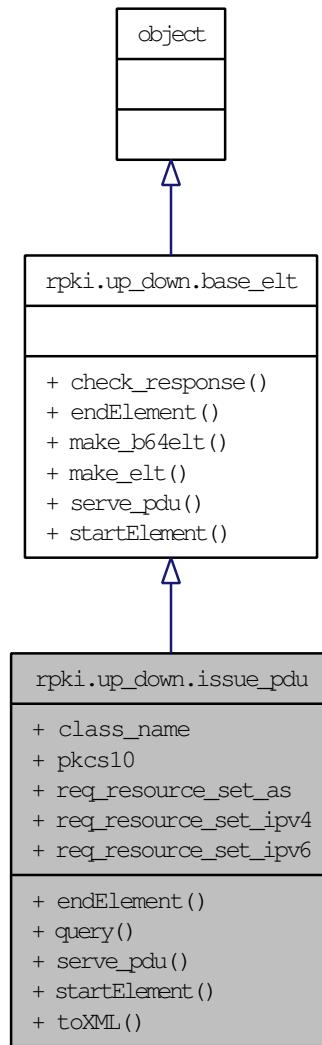
- [up\\_down.py \(3162\)](#)

**11.185 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](#)

### 11.185.1 Detailed Description

Up-Down protocol "issue" PDU.

Definition at line 317 of file up\_down.py.

### 11.185.2 Member Function Documentation

#### 11.185.2.1 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.

#### 11.185.2.2 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.

#### 11.185.2.3 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.

**11.185.2.4 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.

**11.185.2.5 def rpki.up\_down.issue\_pdu.toXML ( *self*)**

Generate payload of "issue" PDU.

Definition at line 340 of file up\_down.py.

**11.185.3 Member Data Documentation****11.185.3.1 rpki.up\_down.issue\_pdu.class\_name**

Definition at line 327 of file up\_down.py.

**11.185.3.2 rpki.up\_down.issue\_pdu.pkcs10**

Definition at line 337 of file up\_down.py.

**11.185.3.3 rpki.up\_down.issue\_pdu.req\_resource\_set\_as**

Definition at line 328 of file up\_down.py.

**11.185.3.4 rpki.up\_down.issue\_pdu.req\_resource\_set\_ipv4**

Definition at line 329 of file up\_down.py.

**11.185.3.5 rpki.up\_down.issue\_pdu.req\_resource\_set\_ipv6**

Definition at line 330 of file up\_down.py.

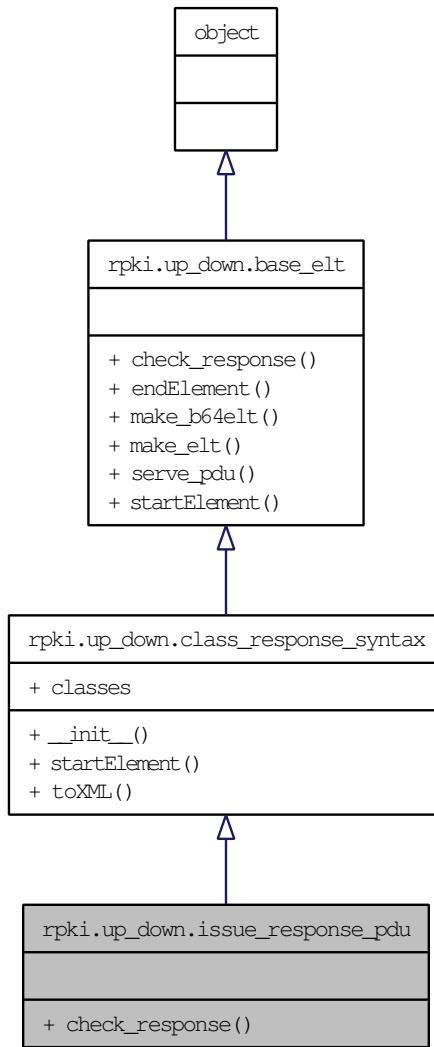
The documentation for this class was generated from the following file:

- [up\\_down.py \(3162\)](#)

**11.186 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](#)

### 11.186.1 Detailed Description

Up-Down protocol "issue\_response" PDU.

Definition at line 431 of file up\_down.py.

### **11.186.2 Member Function Documentation**

#### **11.186.2.1 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:

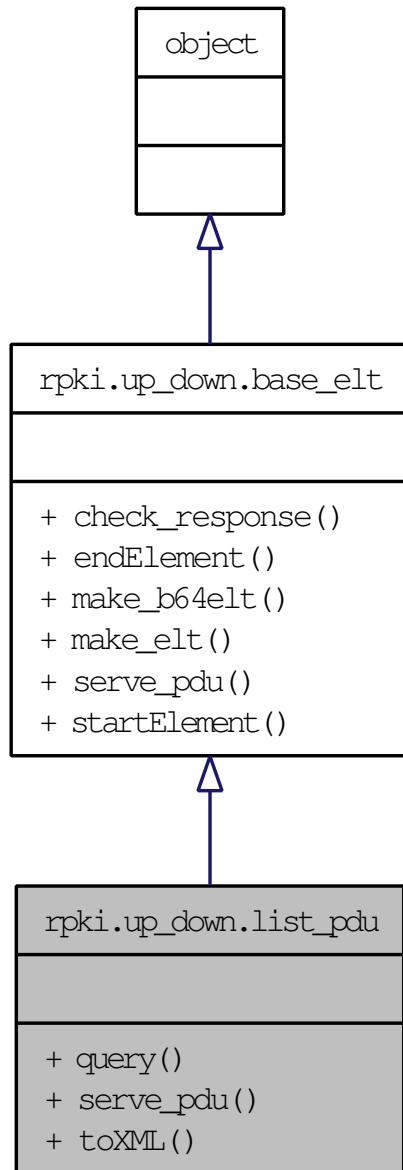
- [up\\_down.py \(3162\)](#)

### **11.187 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](#)

### 11.187.1 Detailed Description

Up-Down protocol "list" PDU.

Definition at line 231 of file up\_down.py.

### 11.187.2 Member Function Documentation

#### 11.187.2.1 def rpki.up\_down.list\_pdu.query (*cls, parent, cb, eb*)

Send a "list" query to parent.

Definition at line 273 of file up\_down.py.

#### 11.187.2.2 def rpki.up\_down.list\_pdu.serve\_pdu (*self, q\_msg, r\_msg, child, callback, errback*)

Serve one "list" PDU.

Reimplemented from [rpki.up\\_down.base\\_elt](#).

Reimplemented in [rootd.list\\_pdu](#).

Definition at line 240 of file up\_down.py.

#### 11.187.2.3 def rpki.up\_down.list\_pdu.toXML (*self*)

Generate (empty) payload of "list" PDU.

Definition at line 236 of file up\_down.py.

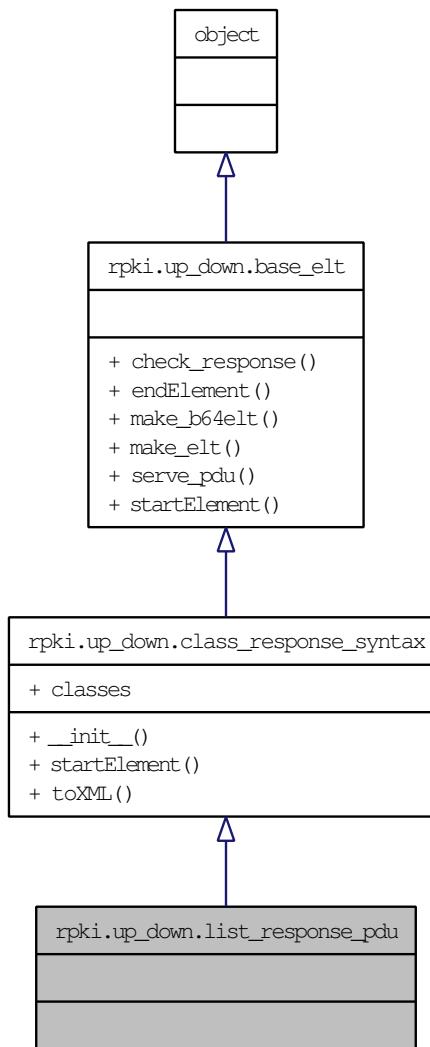
The documentation for this class was generated from the following file:

- [up\\_down.py \(3162\)](#)

## 11.188 rpki.up\_down.list\_response\_pdu Class Reference

Inherits [rpki::up\\_down::class\\_response\\_syntax](#).

Collaboration diagram for rpki.up\_down.list\_response\_pdu:



### 11.188.1 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:

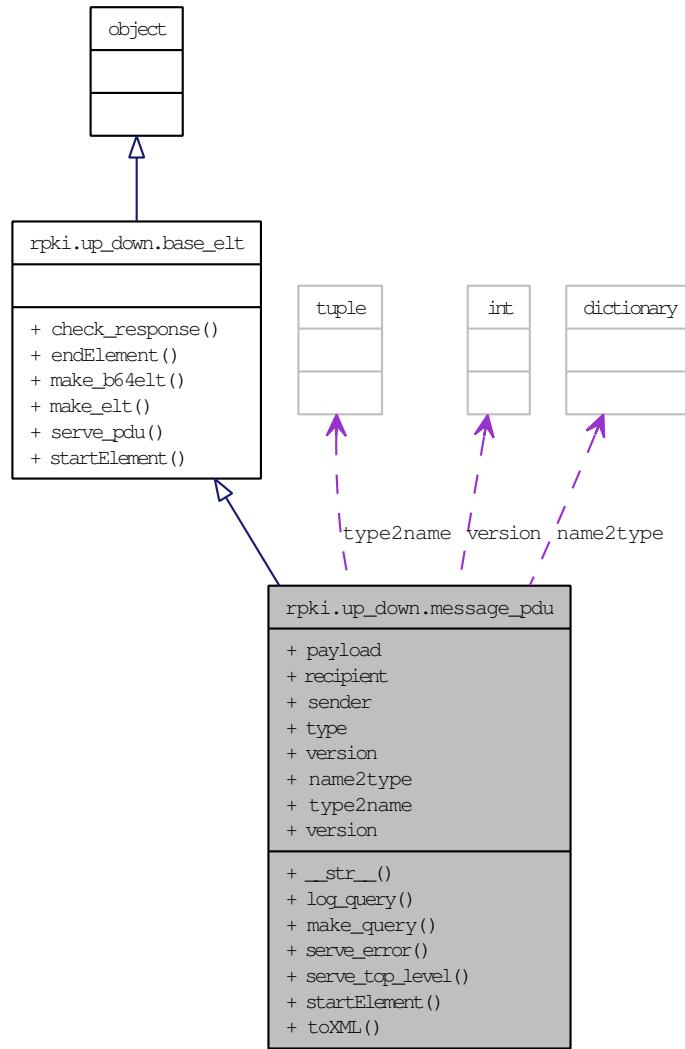
- [up\\_down.py \(3162\)](#)

## 11.189 rpkি.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

### 11.189.1 Detailed Description

Up-Down protocol message wrapper PDU.

Definition at line 571 of file up\_down.py.

### 11.189.2 Member Function Documentation

#### 11.189.2.1 def rpk.up\_down.message\_pdu.[\\_\\_str\\_\\_](#) (*self*)

Convert a message PDU to a string.

Definition at line 613 of file up\_down.py.

#### 11.189.2.2 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.

**11.189.2.3 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.

**11.189.2.4 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.

**11.189.2.5 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.

**11.189.2.6 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.

**11.189.2.7 def rpki.up\_down.message\_pdu.toXML (*self*)**

Generate payload of message PDU.

Definition at line 589 of file up\_down.py.

### 11.189.3 Member Data Documentation

#### 11.189.3.1 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.

#### 11.189.3.2 rpkid.up\_down.message\_pdu.payload

Definition at line 610 of file up\_down.py.

#### 11.189.3.3 rpkid.up\_down.message\_pdu.recipient

Definition at line 608 of file up\_down.py.

#### 11.189.3.4 rpkid.up\_down.message\_pdu.sender

Definition at line 607 of file up\_down.py.

#### 11.189.3.5 rpkid.up\_down.message\_pdu.type

Definition at line 609 of file up\_down.py.

#### 11.189.3.6 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.

#### **11.189.3.7 rpki.up\_down.message\_pdu.version**

Definition at line 606 of file up\_down.py.

#### **11.189.3.8 int rpki.up\_down.message\_pdu.version = 1 [static]**

Definition at line 576 of file up\_down.py.

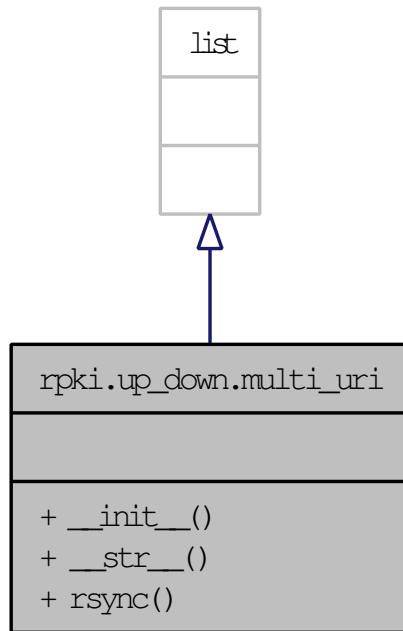
The documentation for this class was generated from the following file:

- [up\\_down.py \(3162\)](#)

### **11.190 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](#)

### 11.190.1 Detailed Description

Container for a set of URIs.

Definition at line 95 of file up\_down.py.

### 11.190.2 Member Function Documentation

#### 11.190.2.1 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.

**11.190.2.2 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.

**11.190.2.3 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:

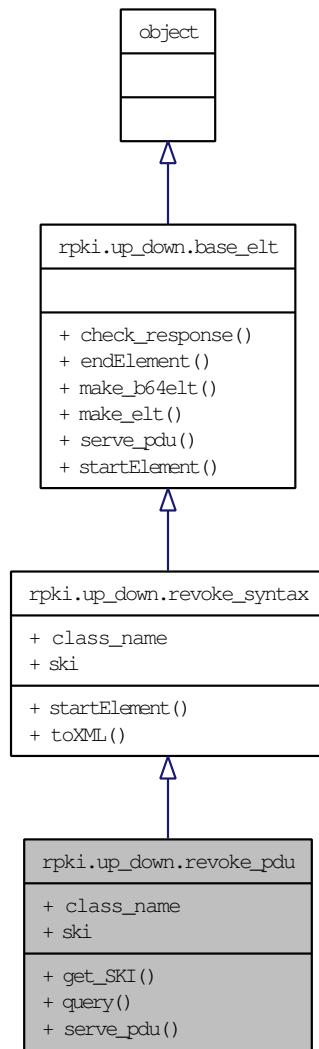
- [up\\_down.py \(3162\)](#)

**11.191 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`

### 11.191.1 Detailed Description

Up-Down protocol "revoke" PDU.

Definition at line 458 of file up\_down.py.

### 11.191.2 Member Function Documentation

#### 11.191.2.1 def rpk.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.

#### 11.191.2.2 def rpk.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.

#### 11.191.2.3 def rpk.up\_down.revoke\_pdu.serve\_pdu (*self, q\_msg, r\_msg, child, cb, eb*)

Serve one revoke request PDU.

Reimplemented from [rpk.up\\_down.base\\_elt](#).

Reimplemented in [rootd.revoke\\_pdu](#).

Definition at line 467 of file up\_down.py.

**11.191.3 Member Data Documentation****11.191.3.1 rpki.up\_down.revoke\_pdu.class\_name**

Reimplemented from [rpki.up\\_down.revoke\\_syntax](#).

Definition at line 493 of file `up_down.py`.

**11.191.3.2 rpki.up\_down.revoke\_pdu.ski**

Reimplemented from [rpki.up\\_down.revoke\\_syntax](#).

Definition at line 494 of file `up_down.py`.

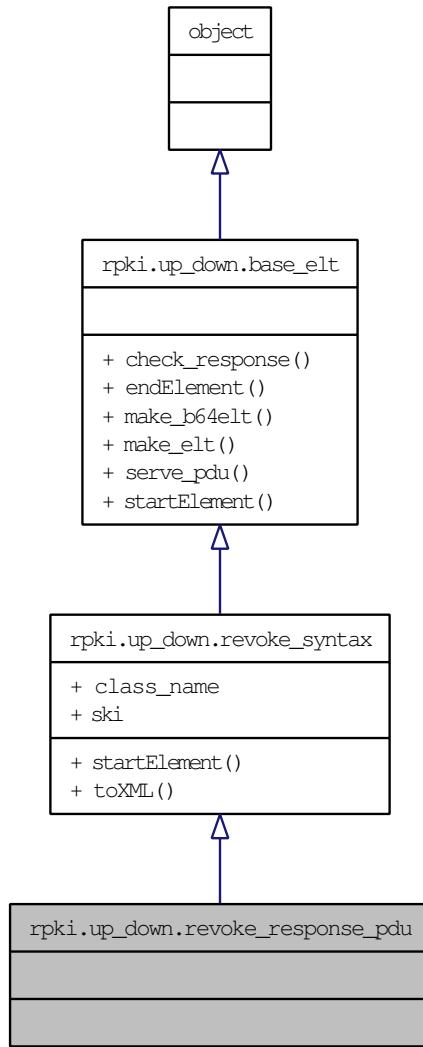
The documentation for this class was generated from the following file:

- [up\\_down.py \(3162\)](#)

**11.192 rpki.up\_down.revoke\_response\_pdu Class Reference**

Inherits [rpki::up\\_down::revoke\\_syntax](#).

Collaboration diagram for rpk.up\_down.revocate\_response\_pdu:



### 11.192.1 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:

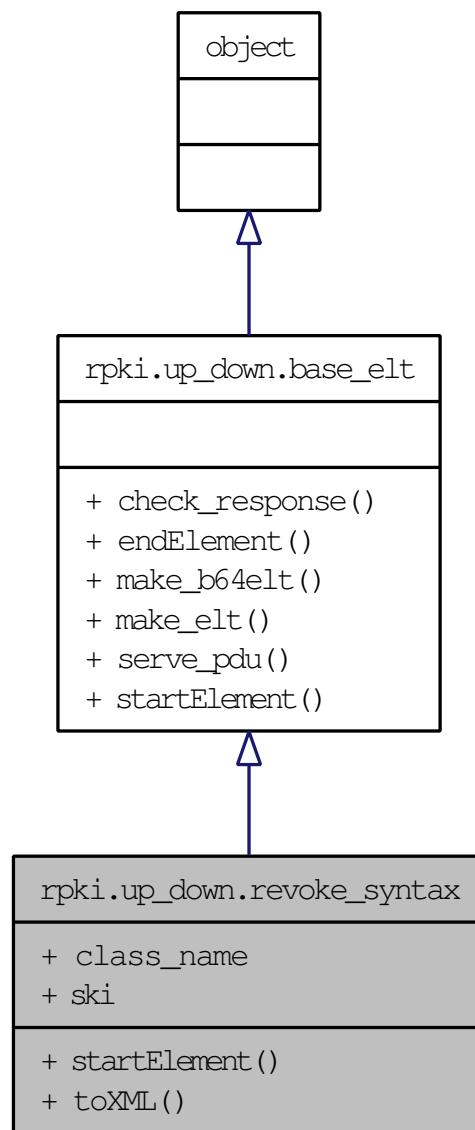
- [up\\_down.py \(3162\)](#)

## 11.193 rpkid.up\_down.revoke\_syntax Class Reference

Inherits [rpkid::up\\_down::base\\_elt](#).

Inherited by [rpkid.up\\_down.revoke\\_pdu](#), and [rpkid.up\\_down.revoke\\_response\\_pdu](#).

Collaboration diagram for rpkid.up\_down.revoke\_syntax:



## Public Member Functions

- def [startElement](#)
- def [toXML](#)

## Public Attributes

- [class\\_name](#)
- [ski](#)

### 11.193.1 Detailed Description

Syntax for Up-Down protocol "revocate" and "revocate\_response" PDUs.

Definition at line 444 of file up\_down.py.

### 11.193.2 Member Function Documentation

#### 11.193.2.1 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.

#### 11.193.2.2 def rpki.up\_down.revocate\_syntax.toXML (*self*)

Generate payload of "revocate" PDU.

Definition at line 454 of file up\_down.py.

### 11.193.3 Member Data Documentation

#### 11.193.3.1 rpki.up\_down.revocate\_syntax.class\_name

Reimplemented in [rpki.up\\_down.revocate\\_pdu](#).

Definition at line 451 of file up\_down.py.

**11.193.3.2 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:

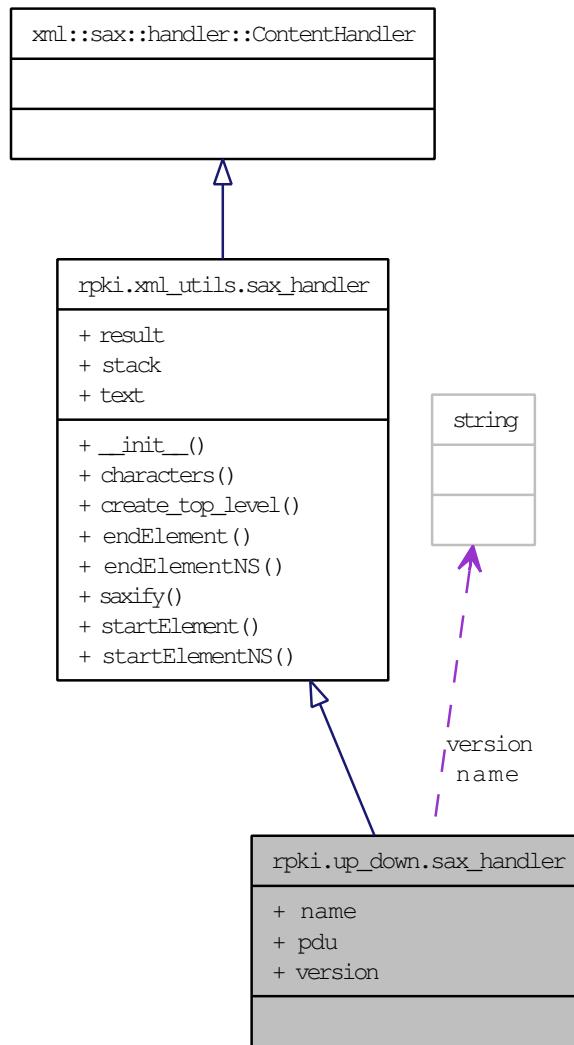
- [up\\_down.py \(3162\)](#)

**11.194 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"

### 11.194.1 Detailed Description

SAX handler for Up-Down protocol.

Definition at line 676 of file up\_down.py.

### 11.194.2 Member Data Documentation

#### 11.194.2.1 string rpki.up\_down.sax\_handler.name = "message" [static]

Definition at line 682 of file up\_down.py.

#### 11.194.2.2 rpki.up\_down.sax\_handler.pdu = message\_pdu [static]

Reimplemented in [rootd.sax\\_handler](#).

Definition at line 681 of file up\_down.py.

#### 11.194.2.3 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:

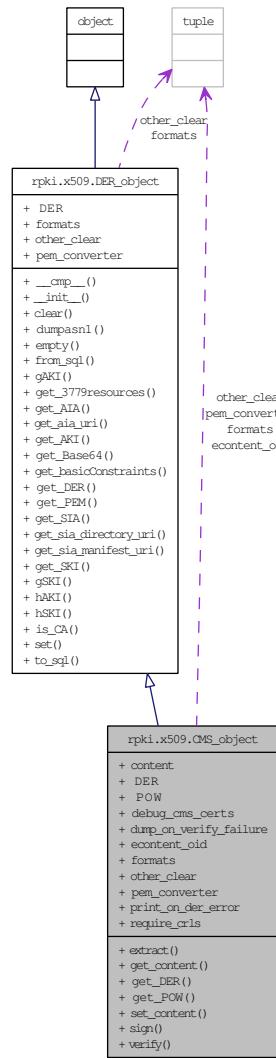
- [up\\_down.py \(3162\)](#)

## 11.195 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.*

### 11.195.1 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.

### 11.195.2 Member Function Documentation

#### 11.195.2.1 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.

#### 11.195.2.2 def rpkix509.CMS\_object.get\_content (*self*)

Get the inner content of this CMS\_object.

Definition at line 797 of file x509.py.

#### 11.195.2.3 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.

**11.195.2.4 def rpkix509.CMS\_object.get\_POW (*self*)**

Get the POW value of this CMS\_object.

Definition at line 788 of file x509.py.

**11.195.2.5 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.

**11.195.2.6 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.

**11.195.2.7 def rpkix509.CMS\_object.verify (*self, ta*)**

Verify CMS wrapper and store inner content.

Definition at line 812 of file x509.py.

**11.195.3 Member Data Documentation****11.195.3.1 rpkix509.CMS\_object.content**

Reimplemented in [rpkix509.DER\\_CMS\\_object](#), and [rpkix509.XML\\_CMS\\_object](#).

Definition at line 810 of file x509.py.

**11.195.3.2 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.

**11.195.3.3 rpki.x509.CMS\_object.DER**

DER value of this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 784 of file x509.py.

**11.195.3.4 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.

**11.195.3.5 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.

**11.195.3.6 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.

**11.195.3.7 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.

**11.195.3.8 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.

**11.195.3.9 rpkix509.CMS\_object.POW**

Definition at line 794 of file x509.py.

**11.195.3.10 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.

**11.195.3.11 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.

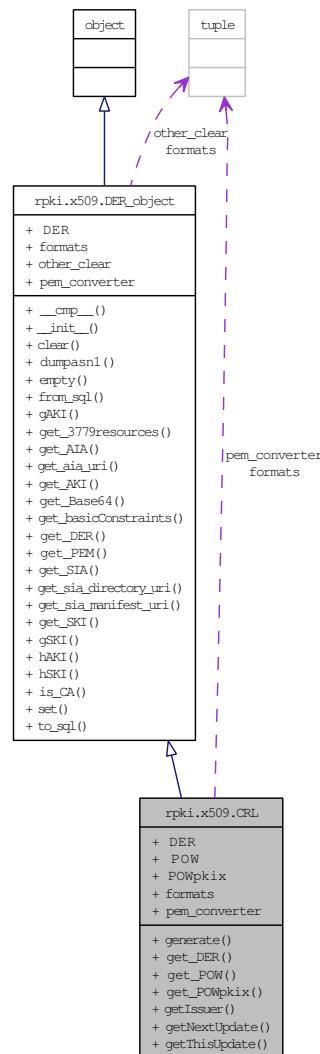
The documentation for this class was generated from the following file:

- x509.py (3107)

## 11.196 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.*

#### 11.196.1 Detailed Description

Class to hold a Certificate Revocation List.

Definition at line 1140 of file x509.py.

#### 11.196.2 Member Function Documentation

##### 11.196.2.1 def rPKI.x509.CRL.generate ( *cls, keypair, issuer, serial, thisUpdate, nextUpdate, revokedCertificates, version = 1, digestType = "sha256WithRSAEncryption"* )

Generate a new CRL.

Definition at line 1196 of file x509.py.

**11.196.2.2 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.

**11.196.2.3 def rpki.x509.CRL.get\_POW ( *self* )**

Get the POW value of this CRL.

Definition at line 1163 of file x509.py.

**11.196.2.4 def rpki.x509.CRL.get\_POWpkix ( *self* )**

Get the POW.pkix value of this CRL.

Definition at line 1172 of file x509.py.

**11.196.2.5 def rpki.x509.CRL.getIssuer ( *self* )**

Get issuer value of this CRL.

Definition at line 1191 of file x509.py.

**11.196.2.6 def rpki.x509.CRL.getNextUpdate ( *self* )**

Get nextUpdate value from this CRL.

Definition at line 1187 of file x509.py.

**11.196.2.7 def rpki.x509.CRL.getThisUpdate ( *self* )**

Get thisUpdate value from this CRL.

Definition at line 1183 of file x509.py.

**11.196.3 Member Data Documentation****11.196.3.1 rpki.x509.CRL.DER**

DER value of this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 1156 of file x509.py.

**11.196.3.2 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.

**11.196.3.3 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.

**11.196.3.4 rpki.x509.CRL.POW**

Definition at line 1169 of file x509.py.

### 11.196.3.5 rpki.x509.CRL.PO Wpkix

Definition at line 1180 of file x509.py.

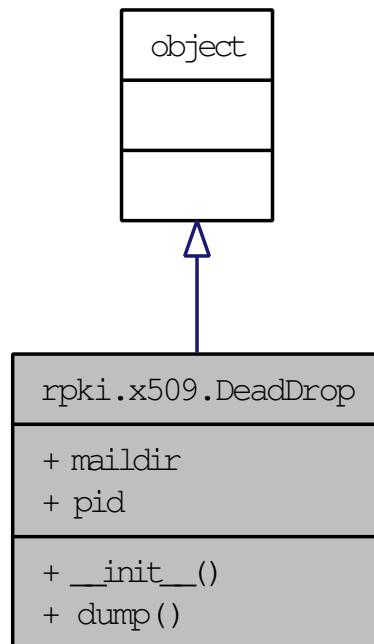
The documentation for this class was generated from the following file:

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

## 11.197 rpki.x509.DeadDrop Class Reference

Inherits [object](#).

Collaboration diagram for rpki.x509.DeadDrop:



### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [dump](#)

### Public Attributes

- [maildir](#)
- [pid](#)

#### 11.197.1 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.

#### 11.197.2 Member Function Documentation

##### 11.197.2.1 def rPKI.x509.DeadDrop.\_\_init\_\_ (*self, name*)

Definition at line 1043 of file x509.py.

##### 11.197.2.2 def rPKI.x509.DeadDrop.dump (*self, obj*)

Definition at line 1047 of file x509.py.

#### 11.197.3 Member Data Documentation

##### 11.197.3.1 rPKI.x509.DeadDrop.maildir

Definition at line 1044 of file x509.py.

##### 11.197.3.2 rPKI.x509.DeadDrop.pid

Definition at line 1045 of file x509.py.

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

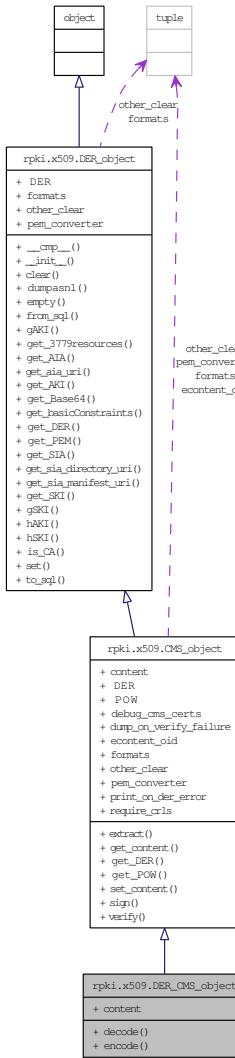
- [x509.py \(3107\)](#)

## 11.198 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](#)

#### 11.198.1 Detailed Description

Class to hold CMS objects with DER-based content.

Definition at line 950 of file x509.py.

#### 11.198.2 Member Function Documentation

##### 11.198.2.1 def rpki.x509.DER\_CMS\_object.decode (*self, der*)

Decode DER and set inner content.

Definition at line 959 of file x509.py.

##### 11.198.2.2 def rpki.x509.DER\_CMS\_object.encode (*self*)

Encode inner content for signing.

Definition at line 955 of file x509.py.

#### 11.198.3 Member Data Documentation

##### 11.198.3.1 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:

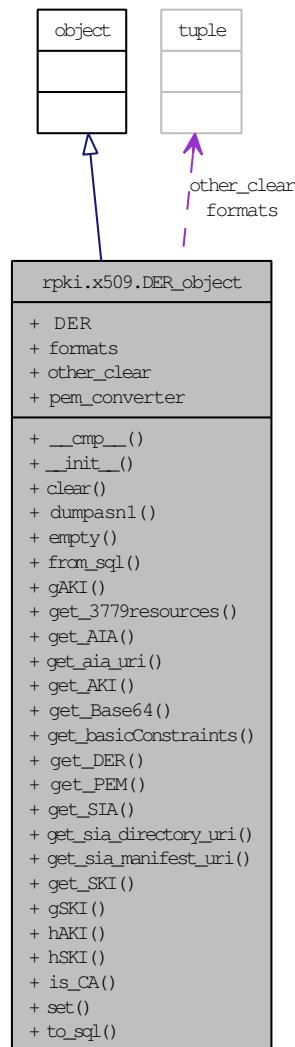
- [x509.py \(3107\)](#)

## 11.199 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.*

### 11.199.1 Detailed Description

Virtual class to hold a generic DER object.

Definition at line 117 of file x509.py.

### 11.199.2 Member Function Documentation

#### 11.199.2.1 def rpkix509.DER\_object.\_\_cmp\_\_ (*self, other*)

Compare two DER-encoded objects.

Definition at line 212 of file x509.py.

#### 11.199.2.2 def rpkix509.DER\_object.\_\_init\_\_ (*self, kw*)

Initialize a DER\_object.

Definition at line 150 of file x509.py.

#### 11.199.2.3 def rpkix509.DER\_object.clear (*self*)

Make this object empty.

Definition at line 143 of file x509.py.

#### 11.199.2.4 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.

**11.199.2.5 def rpki.x509.DER\_object.empty ( *self* )**

Test whether this object is empty.

Definition at line 134 of file x509.py.

**11.199.2.6 def rpki.x509.DER\_object.from\_sql ( *cls*, *x* )**

Convert from SQL storage format.

Definition at line 333 of file x509.py.

**11.199.2.7 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.

**11.199.2.8 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.

**11.199.2.9 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.

**11.199.2.10 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.

**11.199.2.11 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.

**11.199.2.12 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.

**11.199.2.13 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.

**11.199.2.14 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.

**11.199.2.15 def rpki.x509.DER\_object.get\_PEM ( *self* )**

Get the PEM representation of this object.

Definition at line 208 of file x509.py.

**11.199.2.16 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.

**11.199.2.17 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.

**11.199.2.18 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.

**11.199.2.19 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.

**11.199.2.20 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.

**11.199.2.21 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.

**11.199.2.22 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.

**11.199.2.23 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.

**11.199.2.24 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.

**11.199.2.25 def rpki.x509.DER\_object.to\_sql ( *self* )**

Convert to SQL storage format.

Definition at line 337 of file x509.py.

**11.199.3 Member Data Documentation****11.199.3.1 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.

**11.199.3.2 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.

**11.199.3.3 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.

**11.199.3.4 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](#).

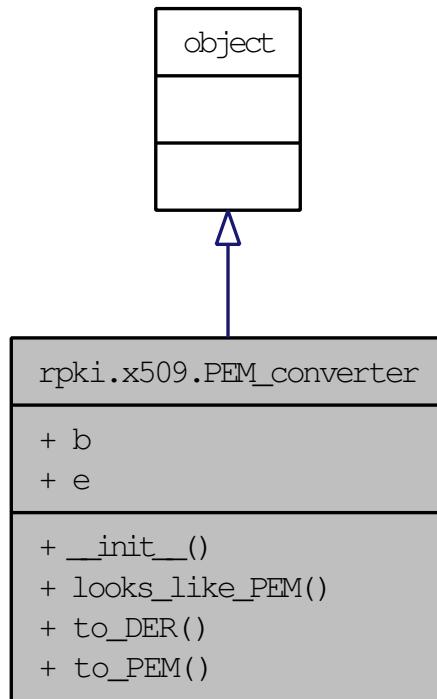
The documentation for this class was generated from the following file:

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

## 11.200 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](#)

#### 11.200.1 Detailed Description

Convert between DER and PEM encodings for various kinds of ASN.1 data.

Definition at line 62 of file x509.py.

#### 11.200.2 Member Function Documentation

##### 11.200.2.1 def rpkix509.PEM\_converter.\_\_init\_\_ (*self*, *kind*)

Initialize PEM\_converter.

Definition at line 67 of file x509.py.

##### 11.200.2.2 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.

##### 11.200.2.3 def rpkix509.PEM\_converter.to\_DER (*self*, *pem*)

Convert from PEM to DER.

Definition at line 81 of file x509.py.

**11.200.2.4 def rpki.x509.PEM\_converter.to\_PEM ( *self*, *der*)**

Convert from DER to PEM.

Definition at line 94 of file x509.py.

**11.200.3 Member Data Documentation****11.200.3.1 rpki.x509.PEM\_converter.b**

Definition at line 71 of file x509.py.

**11.200.3.2 rpki.x509.PEM\_converter.e**

Definition at line 72 of file x509.py.

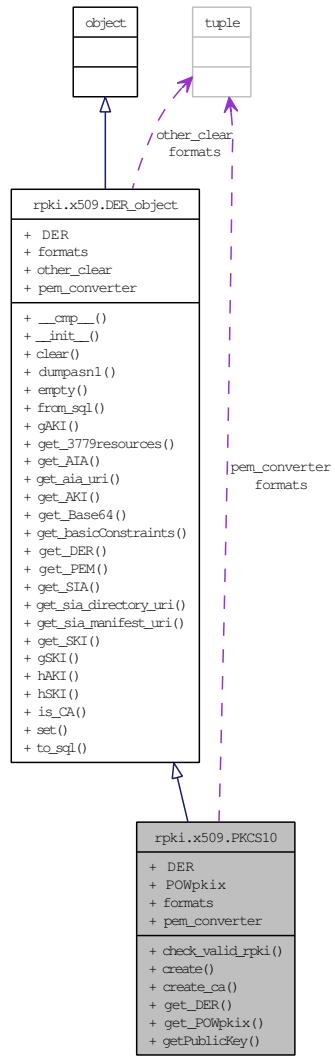
The documentation for this class was generated from the following file:

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

**11.201 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.*

### 11.201.1 Detailed Description

Class to hold a PKCS #10 request.

Definition at line 534 of file x509.py.

### 11.201.2 Member Function Documentation

#### 11.201.2.1 def rpkix509.PKCS10.check\_valid\_rpk ( 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.

#### 11.201.2.2 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.

**11.201.2.3 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.

**11.201.2.4 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.

**11.201.2.5 def rpki.x509.PKCS10.get\_POWpkix ( *self*)**

Get the POW.pkix value of this certification request.

Definition at line 554 of file x509.py.

**11.201.2.6 def rpki.x509.PKCS10.getPublicKey ( *self*)**

Extract the public key from this certification request.

Definition at line 565 of file x509.py.

**11.201.3 Member Data Documentation****11.201.3.1 rpki.x509.PKCS10.DER**

DER value of this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 550 of file x509.py.

**11.201.3.2 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.

**11.201.3.3 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.

**11.201.3.4 rpkix509.PKCS10.POWpkix**

Definition at line 562 of file x509.py.

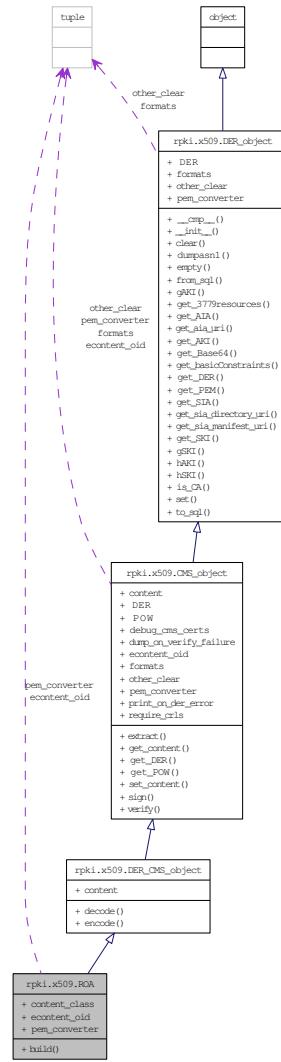
The documentation for this class was generated from the following file:

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

**11.202 rpkix509.ROA Class Reference**

Inherits [rpki::x509::DER\\_CMS\\_object](#).

Collaboration diagram for rpkix509.ROA:



## Public Member Functions

- def `build`

## Static Public Attributes

- `content_class = rpkiroa.RouteOriginAttestation`

- tuple `econtent_oid` = POWify\_OID("id-ct-routeOriginAttestation")
- tuple `pem_converter` = `PEM_converter`("ROUTE ORIGIN ATTESTATION")  
*PEM converter for this object.*

### 11.202.1 Detailed Description

Class to hold a signed ROA.

Definition at line 1007 of file x509.py.

### 11.202.2 Member Function Documentation

#### 11.202.2.1 def rpki.x509.ROA.build ( *cls, asn, ipv4, ipv6, keypair, certs, version = 0* )

Build a ROA.

Definition at line 1017 of file x509.py.

### 11.202.3 Member Data Documentation

#### 11.202.3.1 rpki.x509.ROA.content\_class = rpki.roa.RouteOriginAttestation [static]

Definition at line 1013 of file x509.py.

#### 11.202.3.2 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.

#### 11.202.3.3 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](#).

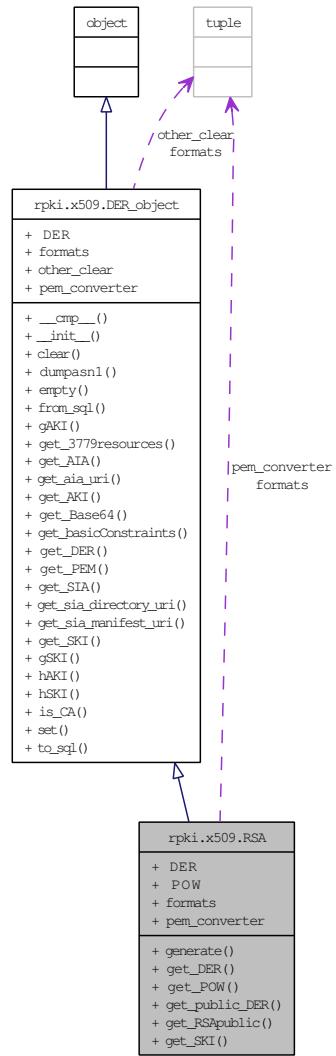
The documentation for this class was generated from the following file:

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

## 11.203 rpki.x509.RSA Class Reference

Inherits [rpki::x509::DER\\_object](#).

Collaboration diagram for rpki.x509.RSA:



## Public Member Functions

- def `generate`
- def `get_DER`
- def `get_POW`
- def `get_public_DER`
- def `get_RSAPublic`
- def `get_SKI`

## Public Attributes

- [DER](#)

*DER value of this object.*

- [POW](#)

## Static Public Attributes

- tuple [formats = \("DER", "POW"\)](#)

*Formats supported in this object.*

- tuple [pem\\_converter = PEM\\_converter\("RSA PRIVATE KEY"\)](#)

*PEM converter for this object.*

### 11.203.1 Detailed Description

Class to hold an RSA key pair.

Definition at line 643 of file x509.py.

### 11.203.2 Member Function Documentation

#### 11.203.2.1 def rpkix509.RSA.generate ( *cls*, *keylength* = 2048)

Generate a new keypair.

Definition at line 673 of file x509.py.

#### 11.203.2.2 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.

**11.203.2.3 def rpki.x509.RSA.get\_POW (*self*)**

Get the POW value of this keypair.

Definition at line 663 of file x509.py.

**11.203.2.4 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.

**11.203.2.5 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.

**11.203.2.6 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.

**11.203.3 Member Data Documentation****11.203.3.1 rpki.x509.RSA.DER**

DER value of this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 659 of file x509.py.

**11.203.3.2 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.

**11.203.3.3 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.

**11.203.3.4 rpki.x509.RSA.POW**

Definition at line 669 of file x509.py.

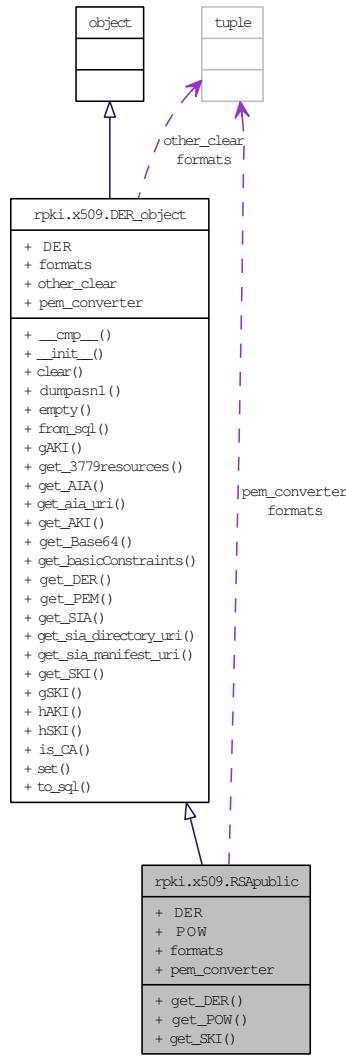
The documentation for this class was generated from the following file:

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

**11.204 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.*

### 11.204.1 Detailed Description

Class to hold an RSA public key.

Definition at line 692 of file x509.py.

### 11.204.2 Member Function Documentation

#### 11.204.2.1 def rpkix509.RSAPublic.get\_DER (*self*)

Get the DER value of this public key.

Reimplemented from [rpkix509.DER\\_object](#).

Definition at line 700 of file x509.py.

#### 11.204.2.2 def rpkix509.RSAPublic.get\_POW (*self*)

Get the POW value of this public key.

Definition at line 712 of file x509.py.

**11.204.2.3 def rpkix509.RSAPublic.get\_SKI ( *self* )**

Calculate the SKI of this public key.

Reimplemented from [rpkix509.DER\\_object](#).

Definition at line 721 of file x509.py.

**11.204.3 Member Data Documentation****11.204.3.1 rpkix509.RSAPublic.DER**

DER value of this object.

Reimplemented from [rpkix509.DER\\_object](#).

Definition at line 708 of file x509.py.

**11.204.3.2 tuple rpkix509.RSAPublic.formats = ("DER", "POW")  
[static]**

Formats supported in this object.

Reimplemented from [rpkix509.DER\\_object](#).

Definition at line 697 of file x509.py.

**11.204.3.3 tuple rpkix509.RSAPublic.pem\_converter = PEM\_converter("RSA  
PUBLIC KEY") [static]**

PEM converter for this object.

Reimplemented from [rpkix509.DER\\_object](#).

Definition at line 698 of file x509.py.

**11.204.3.4 rpkix509.RSAPublic.POW**

Definition at line 718 of file x509.py.

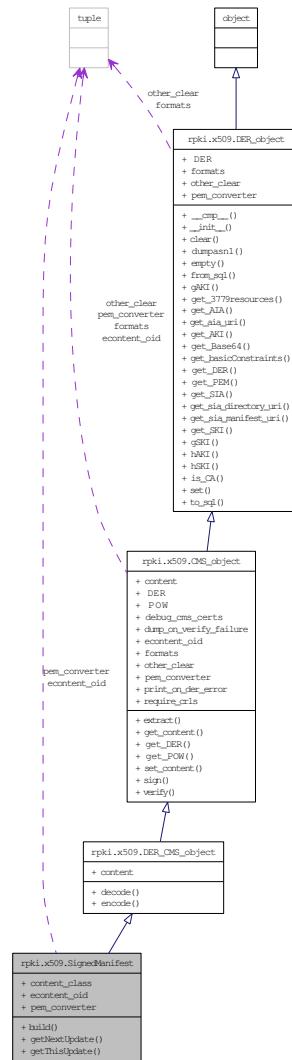
The documentation for this class was generated from the following file:

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

## 11.205 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.*

#### 11.205.1 Detailed Description

Class to hold a signed manifest.

Definition at line 967 of file x509.py.

#### 11.205.2 Member Function Documentation

##### 11.205.2.1 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.

##### 11.205.2.2 def rpkix509.SignedManifest.getNextUpdate ( *self* )

Get nextUpdate value from this manifest.

Definition at line 980 of file x509.py.

**11.205.2.3 def rpkix509.SignedManifest.getThisUpdate (*self*)**

Get thisUpdate value from this manifest.

Definition at line 976 of file x509.py.

**11.205.3 Member Data Documentation****11.205.3.1 rpkix509.SignedManifest.content\_class = rpkixmanifest.Manifest [static]**

Definition at line 973 of file x509.py.

**11.205.3.2 tuple rpkix509.SignedManifest.econtent\_oid = POWify\_OID("id-ct-rpkixManifest") [static]**

Reimplemented from [rpkix509.CMS\\_object](#).

Definition at line 974 of file x509.py.

**11.205.3.3 tuple rpkix509.SignedManifest.pem\_converter = PEM\_converter("RPKI MANIFEST") [static]**

PEM converter for this object.

Reimplemented from [rpkix509.CMS\\_object](#).

Definition at line 972 of file x509.py.

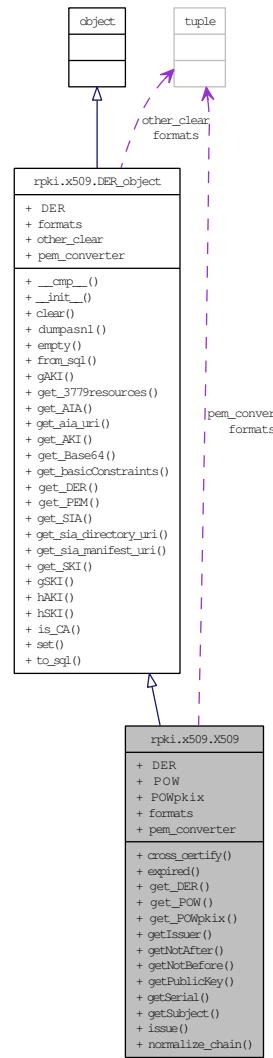
The documentation for this class was generated from the following file:

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

**11.206 rpkix509.X509 Class Reference**

Inherits [rpkix::x509::DER\\_object](#).

Collaboration diagram for rpkix509.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.*

### 11.206.1 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.

### 11.206.2 Member Function Documentation

#### 11.206.2.1 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.

#### 11.206.2.2 def rpki.x509.X509.expired (*self*)

Test whether this certificate has expired.

Definition at line 433 of file x509.py.

#### 11.206.2.3 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.

#### 11.206.2.4 def rpki.x509.X509.get\_POW (*self*)

Get the POW value of this certificate.

Definition at line 389 of file x509.py.

#### 11.206.2.5 def rpki.x509.X509.get\_POWpkix (*self*)

Get the POW.pkix value of this certificate.

Definition at line 398 of file x509.py.

#### 11.206.2.6 def rpki.x509.X509.getIssuer (*self*)

Get the issuer of this certificate.

Definition at line 409 of file x509.py.

**11.206.2.7 def rpki.x509.X509.getNotAfter (*self*)**

Get the expiration time of this certificate.

Definition at line 421 of file x509.py.

**11.206.2.8 def rpki.x509.X509.getNotBefore (*self*)**

Get the inception time of this certificate.

Definition at line 417 of file x509.py.

**11.206.2.9 def rpki.x509.X509.getPublicKey (*self*)**

Extract the public key from this certificate.

Definition at line 429 of file x509.py.

**11.206.2.10 def rpki.x509.X509.getSerial (*self*)**

Get the serial number of this certificate.

Definition at line 425 of file x509.py.

**11.206.2.11 def rpki.x509.X509.getSubject (*self*)**

Get the subject of this certificate.

Definition at line 413 of file x509.py.

**11.206.2.12 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.

**11.206.2.13 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.

**11.206.3 Member Data Documentation****11.206.3.1 rpki.x509.X509.DER**

DER value of this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 382 of file x509.py.

**11.206.3.2 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.

**11.206.3.3 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.

#### **11.206.3.4 rpki.x509.X509.POW**

Definition at line 395 of file x509.py.

#### **11.206.3.5 rpki.x509.X509.POWpkix**

Definition at line 406 of file x509.py.

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

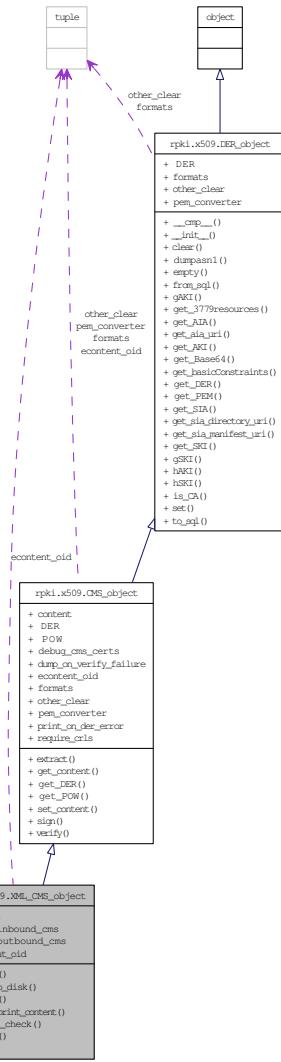
- [x509.py \(3107\)](#)

### **11.207 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")

### 11.207.1 Detailed Description

Class to hold CMS-wrapped XML protocol data.

Definition at line 1058 of file x509.py.

### 11.207.2 Member Function Documentation

#### 11.207.2.1 def rpkix509.XML\_CMS\_object.decode ( *self*, *xml* )

Decode XML and set inner content.

Definition at line 1081 of file x509.py.

#### 11.207.2.2 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.

**11.207.2.3 def rpki.x509.XML\_CMS\_object.encode ( *self* )**

Encode inner content for signing.

Definition at line 1077 of file x509.py.

**11.207.2.4 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.

**11.207.2.5 def rpki.x509.XML\_CMS\_object.schema\_check ( *self* )**

Handle XML RelaxNG schema check.

Definition at line 1089 of file x509.py.

**11.207.2.6 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.

**11.207.2.7 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.

### 11.207.3 Member Data Documentation

#### 11.207.3.1 rpki.x509.XML\_CMS\_object.content

Reimplemented from [rpki.x509.CMS\\_object](#).

Definition at line 1083 of file x509.py.

#### 11.207.3.2 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.

#### 11.207.3.3 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.

#### 11.207.3.4 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:

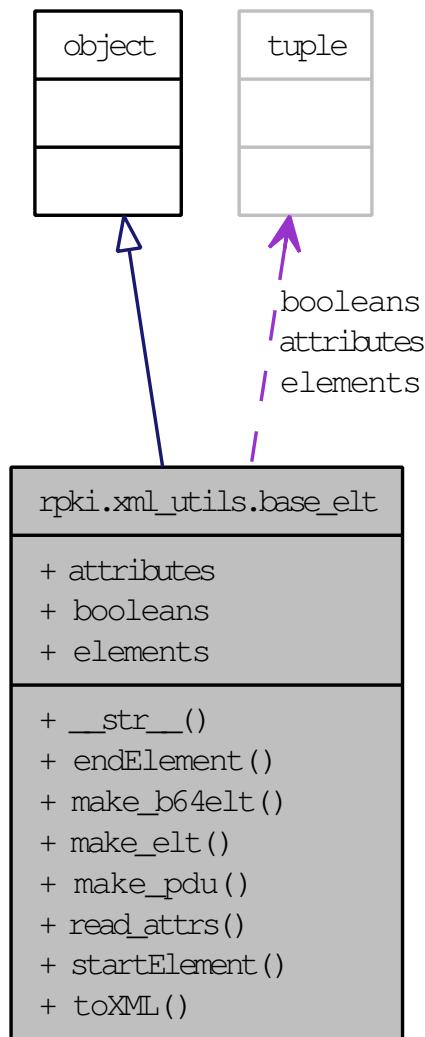
- [x509.py \(3107\)](#)

## 11.208 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 [readAttrs](#)
- 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.*

### 11.208.1 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`.

### 11.208.2 Member Function Documentation

#### 11.208.2.1 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`.

#### 11.208.2.2 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`.

#### 11.208.2.3 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`.

#### 11.208.2.4 def rpki.xml\_utils.base\_elt.make\_elt (*self*)

XML element constructor.

Definition at line 178 of file `xml_utils.py`.

#### 11.208.2.5 def rpki.xml\_utils.base\_elt.make\_pdu (*cls*, *kargs*)

Generic PDU constructor.

Definition at line 208 of file `xml_utils.py`.

#### 11.208.2.6 def rpki.xml\_utils.base\_elt.read\_attrs (*self*, *attrs*)

Template-driven attribute reader.

Definition at line 166 of file `xml_utils.py`.

#### 11.208.2.7 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`.

#### 11.208.2.8 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`.

### 11.208.3 Member Data Documentation

#### 11.208.3.1 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`.

#### 11.208.3.2 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`.

#### 11.208.3.3 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:

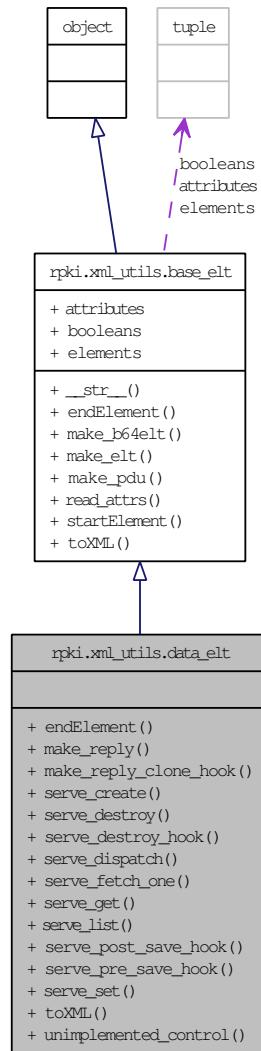
- [xml\\_utils.py \(2836\)](#)

## **11.209 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](#)

### 11.209.1 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`.

### 11.209.2 Member Function Documentation

#### 11.209.2.1 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`.

#### 11.209.2.2 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`.

**11.209.2.3 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`.

**11.209.2.4 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`.

**11.209.2.5 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`.

**11.209.2.6 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`.

**11.209.2.7 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`.

**11.209.2.8 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.

**11.209.2.9 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.

**11.209.2.10 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.

**11.209.2.11 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.

**11.209.2.12 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.

**11.209.2.13 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`.

**11.209.2.14 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`.

**11.209.2.15 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:

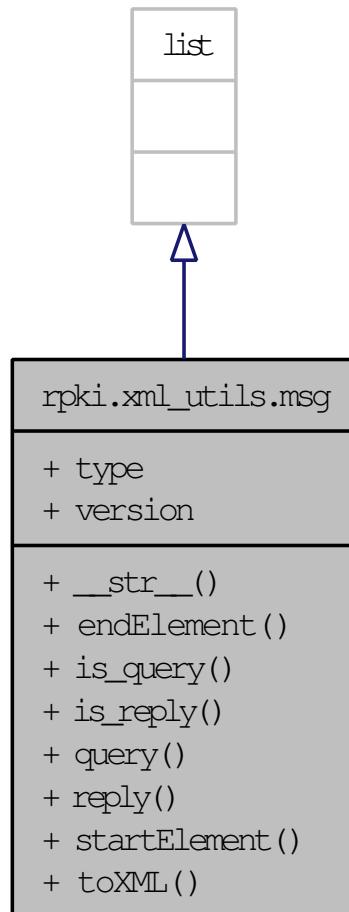
- [xml\\_utils.py \(2836\)](#)

**11.210 rpki.xml\_utils.msg Class Reference**

Inherits list.

Inherited by [rpki.left\\_right.msg](#), and [rpki.publication.msg](#).

Collaboration diagram for rpkixml\_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](#)

### 11.210.1 Detailed Description

Generic top-level PDU.

Definition at line 416 of file `xml_utils.py`.

### 11.210.2 Member Function Documentation

#### 11.210.2.1 def rpkixml\_utils.msg.[\\_\\_str\\_\\_](#) (*self*)

Convert msg object to string.

Definition at line 442 of file `xml_utils.py`.

#### 11.210.2.2 def rpkixml\_utils.msg.[endElement](#) (*self, stack, name, text*)

Handle top-level PDU.

Definition at line 434 of file `xml_utils.py`.

#### 11.210.2.3 def rpkixml\_utils.msg.[is\\_query](#) (*self*)

Is this msg a query?

Definition at line 468 of file `xml_utils.py`.

#### 11.210.2.4 def rpkixml\_utils.msg.[is\\_reply](#) (*self*)

Is this msg a reply?

Definition at line 472 of file `xml_utils.py`.

**11.210.2.5 def rpkixml\_utils.msg.query (*cls, args*)**

Create a query PDU.

Definition at line 455 of file xml\_utils.py.

**11.210.2.6 def rpkixml\_utils.msg.reply (*cls, args*)**

Create a reply PDU.

Definition at line 462 of file xml\_utils.py.

**11.210.2.7 def rpkixml\_utils.msg.startElement (*self, stack, name, attrs*)**

Handle top-level PDU.

Definition at line 421 of file xml\_utils.py.

**11.210.2.8 def rpkixml\_utils.msg.toXML (*self*)**

Generate top-level PDU.

Definition at line 446 of file xml\_utils.py.

**11.210.3 Member Data Documentation****11.210.3.1 rpkixml\_utils.msg.type**

Definition at line 427 of file xml\_utils.py.

**11.210.3.2 rpkixml\_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:

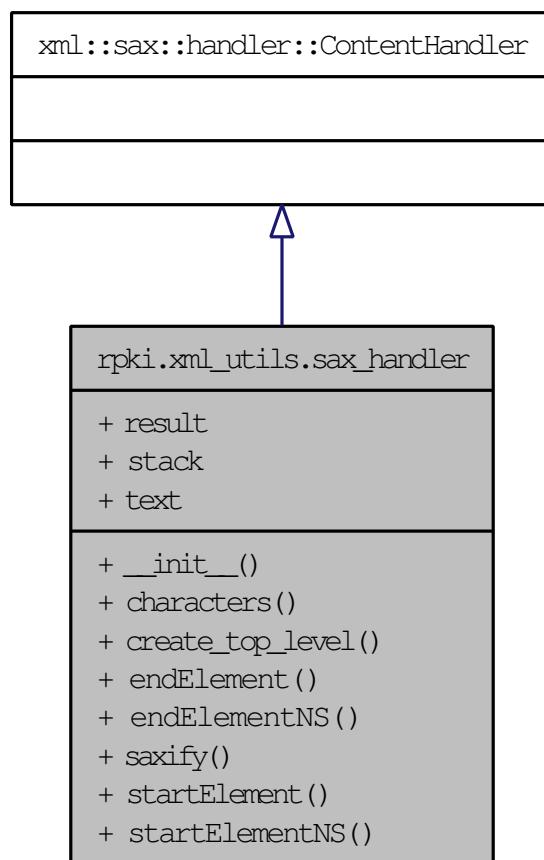
- [xml\\_utils.py \(2836\)](#)

## 11.211 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](#)

#### 11.211.1 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`.

#### 11.211.2 Member Function Documentation

##### 11.211.2.1 def rpk.xml\_utils.sax\_handler.\_\_init\_\_ (*self*)

Initialize SAX handler.

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

**11.211.2.2 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.

**11.211.2.3 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.

**11.211.2.4 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.

**11.211.2.5 def rpkি.xml\_utils.sax\_handler.endElementNS ( *self*, *name*, *qname*)**

Redirect endElementNS() events to endElement().

Definition at line 65 of file xml\_utils.py.

**11.211.2.6 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.

**11.211.2.7 def rpk.xml\_utils.sax\_handler.startElement (*self, name, attrs*)**

Handle startElement() events.

We maintain a stack of nested elements under construction so that we can feed events directly to the current element rather than having to pass them through all the nesting elements.

If the stack is empty, this event is for the outermost element, so we call a virtual method to create the corresponding object and that's the object we'll be returning as our final result.

Definition at line 73 of file xml\_utils.py.

**11.211.2.8 def rpk.xml\_utils.sax\_handler.startElementNS (*self, name, qname, attrs*)**

Redirect startElementNS() events to startElement().

Definition at line 61 of file xml\_utils.py.

**11.211.3 Member Data Documentation****11.211.3.1 rpk.xml\_utils.sax\_handler.result**

Definition at line 97 of file xml\_utils.py.

**11.211.3.2 rpk.xml\_utils.sax\_handler.stack**

Definition at line 59 of file xml\_utils.py.

**11.211.3.3 rpk.xml\_utils.sax\_handler.text**

Definition at line 58 of file xml\_utils.py.

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

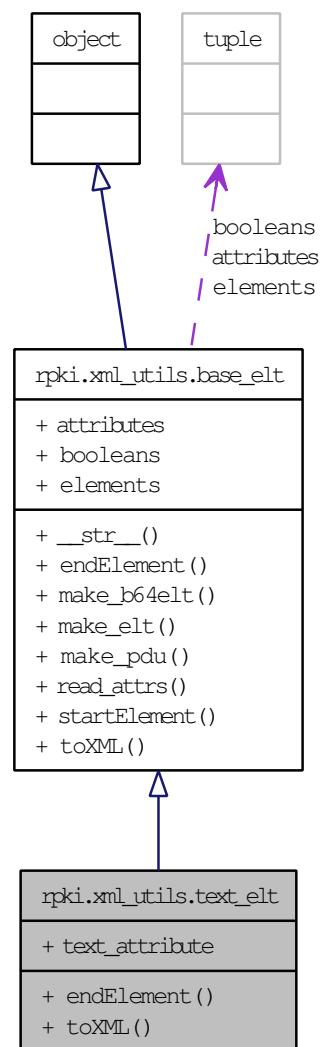
- [xml\\_utils.py \(2836\)](#)

## 11.212 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.*

### 11.212.1 Detailed Description

Virtual base class for XML message elements that contain text.

Definition at line 219 of file `xml_utils.py`.

### 11.212.2 Member Function Documentation

#### 11.212.2.1 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`.

#### 11.212.2.2 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`.

### 11.212.3 Member Data Documentation

#### 11.212.3.1 **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 \(2836\)](#)

## 11.213 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 \(2424\)](#)

## 11.214 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 \(2424\)](#)

## 11.215 TextWrapper Class Reference

Inherited by [irbe\\_cli.UsageWrapper](#).

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

- [irbe\\_cli.py \(3107\)](#)

## 11.216 ContentHandler Class Reference

Inherited by [rpki.xml\\_utils.sax\\_handler](#).

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

- [xml\\_utils.py \(2836\)](#)

## 12 File Documentation

### 12.1 `__doc__.py` File Reference

#### Packages

- package `rpkidoc`

#### 12.1.1 Detailed Description

Documentation source, expressed as Python comments to make Doxygen happy.

##### Id

`__doc__.py.in` 3202 2010-04-14 23:09:34Z sra

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

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

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

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

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

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

Definition in file `__doc__.py`.

## 12.2 \_\_init\_\_.py File Reference

### Packages

- package [rpki](#)

## 12.3 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](#)

## 12.4 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

**12.5 config.py File Reference****Classes**

- class [rpki.config.parser](#)

**Packages**

- package [rpki.config](#)

**12.6 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 `rpkி.exceptions.ChildNotFound`
- class `rpkி.exceptions.ClassNameMismatch`
- class `rpkி.exceptions.ClassNameUnknown`
- class `rpkி.exceptions.ClientNotFound`
- class `rpkி.exceptions.CMSContentNotSet`
- class `rpkி.exceptions.CMSCRLNotSet`
- class `rpkி.exceptions.CMSVerificationFailed`
- class `rpkி.exceptions.DBConsistencyError`
- class `rpkி.exceptions.DEROBJECTConversionError`
- class `rpkி.exceptions.DuplicateObject`
- class `rpkி.exceptions.EmptyPEM`
- class `rpkி.exceptions.EmptyROAPrefixList`
- class `rpkி.exceptions.ForbiddenURI`
- class `rpkி.exceptions.HandleTranslationError`
- class `rpkி.exceptions.HTTPRequestFailed`
- class `rpkி.exceptions.HTTPSBadVersion`
- class `rpkி.exceptions.HTTPSClientAborted`
- class `rpkி.exceptions.HTTPSUnexpectedState`
- class `rpkி.exceptions.MissingCMSCRL`
- class `rpkி.exceptions.MissingCMSEcert`
- class `rpkி.exceptions.MultipleTLSEECert`
- class `rpkி.exceptions.MustBePrefix`
- class `rpkி.exceptions.NoActiveCA`
- class `rpkيء..exceptions.NoCoveringCertForROA`
- class `rpkيء..exceptions.NoObjectAtURI`
- class `rpkيء..exceptions.NotACertificateChain`
- class `rpkيء..exceptions.NotFound`
- class `rpkيء..exceptions.NotImplementedYet`
- class `rpkيء.exceptions.NotInDatabase`
- class `rpkيء.exceptions.ReceivedTLSACert`
- class `rpkيء..exceptions.RPKI_Exception`
- class `rpkيء.exceptions.ServerShuttingDown`
- class `rpkيء.exceptions.SKIMismatch`
- class `rpkيء.exceptions.SubprocessError`
- class `rpkيء.exceptions.TLSValidation`
- class `rpkيء.exceptions.UnexpectedCMSCerts`
- class `rpkيء.exceptions.UnexpectedCMSCRLs`
- class `rpkيء.exceptions.UnparsableCMSDER`
- class `rpkيء.exceptions.UpstreamError`
- class `rpkيء.exceptions.WrongEContentType`

## Packages

- package [rpki.exceptions](#)

## 12.7 https.py File Reference

### Classes

- class [rpki.https.caller](#)
- class [rpki.https.http\\_client](#)
- class [rpki.https.http\\_listener](#)
- class [rpki.https.http\\_message](#)
- class [rpki.https.http\\_queue](#)
- class [rpki.https.http\\_request](#)
- class [rpki.https.http\\_response](#)
- class [rpki.https.http\\_server](#)
- class [rpki.https.http\\_stream](#)

### Packages

- package [rpki.https](#)

### Functions

- def [rpki::https.build\\_https\\_ta\\_cache](#)
- def [rpki::https.client](#)
- def [rpki::https.log\\_method](#)
- def [rpki::https.server](#)

### Variables

- dictionary [rpki::https.client\\_queues](#) = {}  
*Map of (host, port) tuples to http\_queue objects.*
- [rpki::https.debug\\_http](#) = False  
*Verbose chatter about HTTP streams.*
- [rpki::https.debug\\_tls\\_certs](#) = False  
*Verbose chatter about TLS certificates.*
- tuple [rpki::https.default\\_client\\_timeout](#) = [rpki.sundial.timedelta](#)(minutes = 15)  
*Default HTTP client connection timeout.*

- tuple `rpkি::https.default_http_version` = (1, 0)  
*Preferred HTTP version.*
- tuple `rpkি::https.default_server_timeout` = `rpkি.sundial.timedelta(minutes = 20)`  
*Default HTTP server connection timeouts.*
- string `rpkি::https.rpki_content_type` = "application/x-rpki"  
*HTTP content type used for all RPKI messages.*
- tuple `rpkি::https.supported_address_families` = (socket.AF\_INET, socket.AF\_INET6)  
*IP address families to support.*
- `rpkি::https.want_persistent_client` = False  
*Whether we want persistent HTTP client streams, when server also supports them.*
- `rpkি::https.want_persistent_server` = False  
*Whether we want persistent HTTP server streams, when client also supports them.*

## 12.8 ipaddrs.py File Reference

### Classes

- class `rpkি.ipaddrs.v4addr`
- class `rpkি.ipaddrs.v6addr`

### Packages

- package `rpkি.ipaddrs`

## 12.9 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` = `rpkid.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

## 12.10 `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.bpk_i_ta` = `rpkix509.X509`(Auto\_file = cfg.get("bpki-ta"))
- tuple `irdbd.cfg` = `rpkiconfig.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` = `rpkix509.X509`(Auto\_file = cfg.get("irdbd-cert"))
- tuple `irdbd.irdbd_key` = `rpkix509.RSA`( Auto\_file = cfg.get("irdbd-key"))
- int `irdbd.port` = 443
- tuple `irdbd.rpkid_cert` = `rpkix509.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"))

## 12.11 `left_right.py` File Reference

### Classes

- class `rpkileft_right.bsc_elt`

- class [rpki.left\\_right.child\\_elt](#)
- class [rpki.left\\_right.cms\\_msg](#)
- class [rpki.left\\_right.data\\_elt](#)
- class [rpki.left\\_right.left\\_right\\_namespace](#)
- class [rpki.left\\_right.list\\_published\\_objects\\_elt](#)
- class [rpki.left\\_right.list\\_received\\_resources\\_elt](#)
- class [rpki.left\\_right.list\\_resources\\_elt](#)
- class [rpki.left\\_right.list\\_roa\\_requests\\_elt](#)
- class [rpki.left\\_right.msg](#)
- class [rpki.left\\_right.parent\\_elt](#)
- class [rpki.left\\_right.report\\_error\\_elt](#)
- class [rpki.left\\_right.repository\\_elt](#)
- class [rpki.left\\_right.sax\\_handler](#)
- class [rpki.left\\_right.self\\_elt](#)

### Packages

- package [rpki.left\\_right](#)

### Variables

- [rpki::left\\_right.enforce\\_strict\\_up\\_down\\_xml\\_sender](#) = False

## 12.12 log.py File Reference

### Classes

- class [rpki.log.logger](#)

### Packages

- package [rpki.log](#)

### Functions

- def [rpki::log.init](#)
- def [rpki::log.set\\_trace](#)
- def [rpki::log.trace](#)
- def [rpki::log.traceback](#)

## Variables

- tuple `rpkி::log.debug` = logger(syslog.LOG\_DEBUG)
- `rpkி::log.enable_trace` = False  
*Whether call tracing is enabled.*
- tuple `rpkி::log.error` = logger(syslog.LOG\_ERR)
- tuple `rpkி::log.info` = logger(syslog.LOG\_INFO)
- tuple `rpkி::log.note` = logger(syslog.LOG\_NOTICE)
- int `rpkி::log.pid` = 0
- string `rpkி::log.tag` = ""
- `rpkி::log.use_syslog` = True  
*Whether to use syslog.*
- tuple `rpkيء::log.warn` = logger(syslog.LOG\_WARNING)

## 12.13 manifest.py File Reference

### Classes

- class `rpkி.manifest.FileAndHash`
- class `rpkيء.manifest.FilesAndHashes`
- class `rpkيء.manifest.Manifest`

### Packages

- package `rpkيء.manifest`

## 12.14 oids.py File Reference

### Packages

- package `rpkيء.oids`

## Variables

- tuple `rpkيء::oids.name2oid` = dict((v, k) for k, v in oid2name.items())  
*Mapping table of string names to OIDs.*
- dictionary `rpkيء::oids.oid2name`  
*Mapping table of OIDs to conventional string names.*

## 12.15 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

## 12.16 publication.py File Reference

### Classes

- class [rpki.publication.certificate\\_elt](#)
- class [rpki.publication.client\\_elt](#)
- class [rpki.publication.cms\\_msg](#)
- class [rpki.publication.config\\_elt](#)
- class [rpki.publication.control\\_elt](#)
- class [rpki.publication.crl\\_elt](#)
- class [rpki.publication.manifest\\_elt](#)
- class [rpki.publication.msg](#)
- class [rpki.publication.publication\\_namespace](#)
- class [rpki.publication.publication\\_object\\_elt](#)
- class [rpki.publication.report\\_error\\_elt](#)
- class [rpki.publication.roa\\_elt](#)
- class [rpki.publication.sax\\_handler](#)

### Packages

- package [rpki.publication](#)

## 12.17 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.*

## 12.18 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 `rpk::resource_set._bs2long`
- def `rpk::resource_set._long2bs`
- def `rpk::resource_set._rsplit`
- def `rpk::resource_set.test1`
- def `rpk::resource_set.test2`

## Variables

- string `rpk::resource_set.inherit_token` = "<inherit>"  
*Token used to indicate inheritance in read and print syntax.*

## 12.19 roa.py File Reference

### Classes

- class `rpk.roa.ROAIPAddress`
- class `rpk.roa.ROAIPAddresses`
- class `rpk.roa.ROAIPAddressFamilies`
- class `rpk.roa.ROAIPAddressFamily`
- class `rpk.roa.RouteOriginAttestation`

### Packages

- package `rpk.roa`

## 12.20 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.rotd_bpki_cert = rpki.x509.X509(Auto_file = cfg.get("rotd-bpki-cert"))`
- tuple `rootd.rotd_bpki_crl = rpki.x509.CRL( Auto_file = cfg.get("rotd-bpki-crl"))`
- tuple `rootd.rotd_bpki_key = rpki.x509.RSA( Auto_file = cfg.get("rotd-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,`

## 12.21 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`

## 12.22 rpkid.py File Reference

### Packages

- package `rpkid`

### Functions

- def `rpkid.main`

### Variables

- string `rpkid.cfg_file` = "rpkid.conf"
- `rpkid.profile` = None

## 12.23 sql.py File Reference

### Classes

- class [rpki.sql.session](#)
- class [rpki.sql.sql\\_persistent](#)
- class [rpki.sql.template](#)

### Packages

- package [rpki.sql](#)

## 12.24 sundial.py File Reference

### Classes

- class [rpki.sundial.datetime](#)
- class [rpki.sundial.timedelta](#)

### Packages

- package [rpki.sundial](#)

### Functions

- def [rpki::sundial.\\_cast](#)
- def [rpki::sundial.now](#)
- def [rpki::sundial.test](#)

## 12.25 up\_down.py File Reference

### Classes

- class [rpki.up\\_down.base\\_elt](#)
- class [rpki.up\\_down.certificate\\_elt](#)
- class [rpki.up\\_down.class\\_elt](#)
- class [rpki.up\\_down.class\\_response\\_syntax](#)
- class [rpki.up\\_down.cms\\_msg](#)
- class [rpki.up\\_down.error\\_response\\_pdu](#)
- class [rpki.up\\_down.issue\\_pdu](#)
- class [rpki.up\\_down.issue\\_response\\_pdu](#)

- class [rpki.up\\_down.list\\_pdu](#)
- class [rpki.up\\_down.list\\_response\\_pdu](#)
- class [rpki.up\\_down.message\\_pdu](#)
- class [rpki.up\\_down.multi\\_uri](#)
- class [rpki.up\\_down.revoke\\_pdu](#)
- class [rpki.up\\_down.revoke\\_response\\_pdu](#)
- class [rpki.up\\_down.revoke\\_syntax](#)
- class [rpki.up\\_down.sax\\_handler](#)

### Packages

- package [rpki.up\\_down](#)

### Variables

- dictionary [rpki::up\\_down.nsmap](#) = { None : xmlns }
- string [rpki::up\\_down.xmlns](#) = "http://www.apnic.net/specs/rescerts/up-down/"

## 12.26 x509.py File Reference

### Classes

- class [rpki.x509.CMS\\_object](#)
- class [rpki.x509.CRL](#)
- class [rpki.x509.DeadDrop](#)
- class [rpki.x509.DER\\_CMS\\_object](#)
- class [rpki.x509.DER\\_object](#)
- class [rpki.x509.PEM\\_converter](#)
- class [rpki.x509.PKCS10](#)
- class [rpki.x509.ROA](#)
- class [rpki.x509.RSA](#)
- class [rpki.x509.RSAPublic](#)
- class [rpki.x509.SignedManifest](#)
- class [rpki.x509.X509](#)
- class [rpki.x509.XML\\_CMS\\_object](#)

### Packages

- package [rpki.x509](#)

## Functions

- def [rpki::x509.\\_find\\_xia\\_uri](#)
- def [rpki::x509.calculate\\_SKI](#)
- def [rpki::x509.POWify\\_OID](#)

## 12.27 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`, 517  
`__add__`  
    `rpkii::sundial::datetime`, 510  
    `rpkii::sundial::timedelta`, 517  
`__call__`  
    `irbe_cli::UsageWrapper`, 153  
    `rpkii::async::iterator`, 173  
    `rpkii::async::sync_wrapper`, 177  
    `rpkii::https::caller`, 252  
    `rpkii::log::logger`, 354  
`__cmp__`  
    `rpkii::async::timer`, 181  
    `rpkii::resource_set::resource_range`,  
        403  
    `rpkii::resource_set::roa_prefix`, 429  
    `rpkii::x509::DER_object`, 581  
`__del__`  
    `rpkii::async::timer`, 181  
`__div__`  
    `rpkii::sundial::timedelta`, 517  
`__doc__.py`, 637  
`__eq__`  
    `rpkii::resource_set::resource_bag`,  
        399  
`__floordiv__`  
    `rpkii::sundial::timedelta`, 517  
`__init__`  
    `pubd::pubd_context`, 155  
    `rpkii::async::gc_summary`, 171  
    `rpkii::async::iterator`, 173  
    `rpkii::async::sync_wrapper`, 177  
    `rpkii::async::timer`, 181  
    `rpkii::cli::Cmd`, 186  
    `rpkii::config::parser`, 191  
    `rpkii::https::caller`, 252  
    `rpkii::https::http_client`, 255  
    `rpkii::https::http_listener`, 261  
    `rpkii::https::http_message`, 264  
    `rpkii::https::http_queue`, 268  
    `rpkii::https::http_request`, 272  
    `rpkii::https::http_response`, 275  
`rpkii::https::http_server`, 278  
`rpkii::https::http_stream`, 284  
`rpkii::log::logger`, 354  
`rpkii::manifest::FileAndHash`, 356  
`rpkii::manifest::FilesAndHashes`, 357  
`rpkii::manifest::Manifest`, 359  
`rpkii::resource_set::resource_bag`,  
    399  
`rpkii::resource_set::resource_range`,  
    403  
`rpkii::resource_set::resource_set`, 415  
`rpkii::resource_set::roa_prefix`, 429  
`rpkii::resource_set::roa_prefix_set`,  
    437  
`rpkii::roa::ROAIPAddress`, 443  
`rpkii::roa::ROAIPAddresses`, 445  
`rpkii::roa::ROAIPAddressFamilies`,  
    446  
`rpkii::roa::ROAIPAddressFamily`,  
    447  
`rpkii::roa::RouteOriginAttestation`,  
    449  
`rpkii::rpki_engine::child_cert_obj`,  
    468  
`rpkii::rpki_engine::publication_-`  
    queue, 473  
`rpkii::rpki_engine::revoked_cert_obj`,  
    476  
`rpkii::rpki_engine::roa_obj`, 480  
`rpkii::rpki_engine::rpkid_context`,  
    488  
`rpkii::sql::session`, 495  
`rpkii::sql::template`, 507  
`rpkii::up_down::class_elt`, 527  
`rpkii::up_down::class_response_-`  
    syntax, 531  
`rpkii::up_down::error_response_pdu`,  
    536  
`rpkii::up_down::multi_uri`, 554  
`rpkii::x509::DeadDrop`, 576  
`rpkii::x509::DER_object`, 581  
`rpkii::x509::PEM_converter`, 588

rpkii::xml\_utils::sax\_handler, 631  
\_\_init\_\_.py(3150), 638  
\_\_mul\_\_  
    rpki::sundial::timedelta, 517  
\_\_ne\_\_  
    rpki::resource\_set::resource\_bag,  
        399  
\_\_neg\_\_  
    rpki::sundial::timedelta, 517  
\_\_new\_\_  
    rpki::ipaddrs::v4addr, 291  
    rpki::ipaddrs::v6addr, 294  
\_\_pos\_\_  
    rpki::sundial::timedelta, 517  
\_\_radd\_\_  
    rpki::sundial::datetime, 510  
    rpki::sundial::timedelta, 517  
\_\_rdiv\_\_  
    rpki::sundial::timedelta, 518  
\_\_repr\_\_  
    rpki::async::iterator, 174  
    rpki::async::timer, 181  
\_\_rfloordiv\_\_  
    rpki::sundial::timedelta, 518  
\_\_rmul\_\_  
    rpki::sundial::timedelta, 518  
\_\_rsub\_\_  
    rpki::sundial::datetime, 510  
    rpki::sundial::timedelta, 518  
\_\_str\_\_  
    rpki::https::http\_message, 264  
    rpki::ipaddrs::v4addr, 291  
    rpki::ipaddrs::v6addr, 294  
    rpki::publication::report\_error\_elt,  
        391  
    rpki::resource\_set::resource\_bag,  
        400  
rpki::resource\_set::resource\_range\_-  
    as, 405  
rpki::resource\_set::resource\_range\_-  
    ip, 408  
rpki::resource\_set::resource\_set, 415  
rpki::resource\_set::roa\_prefix, 429  
rpki::resource\_set::roa\_prefix\_set,  
    437  
rpki::sundial::datetime, 511  
rpkii::up\_down::message\_pdu, 550  
rpkii::up\_down::multi\_uri, 555  
rpki::xml\_utils::base\_elt, 618  
rpki::xml\_utils::msg, 628  
\_\_sub\_\_  
    rpki::sundial::datetime, 511  
    rpki::sundial::timedelta, 518  
\_add  
    rpki::rpki\_engine::publication\_-  
        queue, 473  
\_bs2long  
    rpki::resource\_set, 91  
\_cast  
    rpki::sundial, 96  
\_comm  
    rpki::resource\_set::resource\_set, 415  
\_exceptions\_enabled  
    rpki::sql::session, 496  
\_find\_xia\_uri  
    rpki::x509, 100  
\_long2bs  
    rpki::resource\_set, 91  
\_prefixlen  
    rpki::resource\_set::resource\_range\_-  
        ip, 408  
\_raiseExitNow  
    rpki::async, 69  
\_regexp  
    rpki::config::parser, 193  
\_repl  
    rpki::config::parser, 191  
\_rsplit  
    rpki::resource\_set, 91  
\_wrap\_execute  
    rpki::sql::session, 495  
\_yes\_or\_no\_prompts  
    rpki::cli, 72  
activate  
    rpki::rpki\_engine::ca\_detail\_obj,  
        453  
address  
    rpki::roa::ROAIPAddress, 444  
addresses  
    rpki::roa::ROAIPAddressFamily,  
        448

addressFamily  
    rpki::roa::ROAIPAddressFamily,  
        448

af  
    rpki::https::http\_client, 258

afi  
    rpki::resource\_set::resource\_set\_-  
        ipv4, 425  
    rpki::resource\_set::resource\_set\_-  
        ipv6, 427

argv  
    irbe\_cli, 52

asID  
    rpki::roa::RouteOriginAttestation,  
        449

asn  
    rpki::left\_right::list\_resources\_elt,  
        322  
    rpki::resource\_set::resource\_bag,  
        401  
    rpki::rpki\_engine::roa\_obj, 483

assert\_pristine  
    rpki::sql::session, 495

async.py(3191), 638

asynchat::async\_chat, 103

asyncore::dispatcher, 103

attributes  
    rpki::left\_right::bsc\_elt, 298  
    rpki::left\_right::child\_elt, 304  
    rpki::left\_right::list\_published\_-  
        objects\_elt, 316  
    rpki::left\_right::list\_received\_-  
        resources\_elt, 318  
    rpki::left\_right::list\_resources\_elt,  
        322  
    rpki::left\_right::list\_roa\_requests\_-  
        elt, 324  
    rpki::left\_right::parent\_elt, 332  
    rpki::left\_right::report\_error\_elt, 337  
    rpki::left\_right::repository\_elt, 341  
    rpki::left\_right::self\_elt, 351  
    rpki::publication::client\_elt, 365  
    rpki::publication::config\_elt, 372  
    rpki::publication::publication\_-  
        object\_elt, 388

rpki::publication::report\_error\_elt,  
    392

rpki::xml\_utils::base\_elt, 620

b  
    rpki::x509::PEM\_converter, 589

base\_uri  
    rpki::publication::client\_elt, 365

bits  
    rpki::ipaddrs::v4addr, 292  
    rpki::ipaddrs::v6addr, 294

body  
    rpki::https::http\_message, 266

booleans  
    rpki::left\_right::bsc\_elt, 298  
    rpki::left\_right::child\_elt, 304  
    rpki::left\_right::parent\_elt, 332  
    rpki::left\_right::self\_elt, 351  
    rpki::xml\_utils::base\_elt, 620

bpkি\_cert  
    irbe\_cli::cmd\_elt\_mixin, 116  
    rpki::left\_right::child\_elt, 304  
    rpki::left\_right::repository\_elt, 341  
    rpki::left\_right::self\_elt, 351  
    rpki::publication::client\_elt, 366

bpkি\_cms\_cert  
    irbe\_cli::cmd\_elt\_mixin, 116  
    rpki::left\_right::parent\_elt, 332

bpkি\_cms\_glue  
    irbe\_cli::cmd\_elt\_mixin, 116  
    rpki::left\_right::parent\_elt, 332

bpkি\_crl  
    irbe\_cli::config\_elt, 120

bpkি\_glue  
    irbe\_cli::cmd\_elt\_mixin, 116  
    rpki::left\_right::child\_elt, 304  
    rpki::left\_right::repository\_elt, 341  
    rpki::left\_right::self\_elt, 351  
    rpki::publication::client\_elt, 366

bpkি\_https\_cert  
    irbe\_cli::cmd\_elt\_mixin, 116  
    rpki::left\_right::parent\_elt, 333

bpkি\_https\_glue  
    irbe\_cli::cmd\_elt\_mixin, 116  
    rpki::left\_right::parent\_elt, 333

bpkি\_ta

irdbd, 56  
pubd::pubd\_context, 156  
rootd, 64  
rpki::rpki\_engine::rpkid\_context, 490  
bsc  
    rpki::left\_right::data\_elt, 309  
bscs  
    rpki::left\_right::self\_elt, 347  
buffer  
    rpki::https::http\_stream, 289  
build  
    rpki::x509::ROA, 595  
    rpki::x509::SignedManifest, 605  
build\_https\_ta\_cache  
    pubd::pubd\_context, 155  
    rpki::https, 77  
    rpki::rpki\_engine::rpkid\_context, 488  
ca  
    rpki::rpki\_engine::ca\_detail\_obj, 453  
ca\_cert\_uri  
    rpki::rpki\_engine::ca\_detail\_obj, 457  
ca\_detail  
    rpki::rpki\_engine::child\_cert\_obj, 468  
    rpki::rpki\_engine::revoked\_cert\_obj, 476  
    rpki::rpki\_engine::roa\_obj, 480  
ca\_detail\_id  
    rpki::rpki\_engine::child\_cert\_obj, 470  
    rpki::rpki\_engine::revoked\_cert\_obj, 477  
    rpki::rpki\_engine::roa\_obj, 483  
ca\_details  
    rpki::rpki\_engine::ca\_obj, 461  
ca\_from\_class\_name  
    rpki::left\_right::child\_elt, 302  
ca\_id  
    rpki::rpki\_engine::ca\_detail\_obj, 457  
cache  
    rpki::sql::session, 497  
cache\_clear  
    rpki::sql::session, 495  
calculate\_SKI  
    rpki::x509, 100  
call\_pubd  
    irbe\_cli, 52  
    rpki::left\_right::repository\_elt, 340  
    rpki::rpki\_engine::publication\_queue, 473  
call\_rpkid  
    irbe\_cli, 52  
callback  
    rpki::https::http\_request, 273  
caller\_function  
    rpki::async::iterator, 174  
cancel  
    rpki::async::timer, 181  
cas  
    rpki::left\_right::parent\_elt, 330  
cb  
    rpki::async::sync\_wrapper, 177  
cert  
    rpki::https::http\_client, 258  
    rpki::https::http\_listener, 262  
    rpki::https::http\_queue, 269  
    rpki::rpki\_engine::child\_cert\_obj, 470  
    rpki::rpki\_engine::roa\_obj, 483  
    rpki::up\_down::certificate\_elt, 525  
cert\_url  
    rpki::up\_down::certificate\_elt, 525  
    rpki::up\_down::class\_elt, 528  
certs  
    rpki::up\_down::class\_elt, 528  
cfg  
    irbe\_cli, 52  
    irdbd, 56  
    rootd, 64  
    rpki::config::parser, 193  
cfg\_file  
    irbe\_cli, 53  
    irdbd, 56  
    pubd, 60  
    rootd, 64  
    rpkid, 102

characters  
    rpki::xml\_utils::sax\_handler, 631

check\_allowed\_uri  
    rpki::publication::client\_elt, 364

check\_for\_updates  
    rpki::rpki\_engine::ca\_obj, 461

check\_response  
    rpki::up\_down::base\_elt, 521  
    rpki::up\_down::error\_response\_pdu,  
        536  
    rpki::up\_down::issue\_response\_pdu,  
        544

check\_valid\_rpki  
    rpki::x509::PKCS10, 591

checkpoint  
    rpki::rpki\_engine::rpkid\_context,  
        488

child  
    rpki::rpki\_engine::child\_cert\_obj,  
        468

child\_bpki\_cert  
    rootd, 64

child\_certs  
    rpki::left\_right::child\_elt, 302  
    rpki::rpki\_engine::ca\_detail\_obj,  
        453

child\_id  
    rpki::rpki\_engine::child\_cert\_obj,  
        470

children  
    rpki::left\_right::bsc\_elt, 297  
    rpki::left\_right::self\_elt, 347

chunk\_body  
    rpki::https::http\_stream, 284

chunk\_discard\_crlf  
    rpki::https::http\_stream, 284

chunk\_discard\_trailer  
    rpki::https::http\_stream, 284

chunk\_handler  
    rpki::https::http\_stream, 289

chunk\_header  
    rpki::https::http\_stream, 284

class\_name  
    rpki::up\_down::class\_elt, 528  
    rpki::up\_down::issue\_pdu, 541  
    rpki::up\_down::revoke\_pdu, 558

            rpki::up\_down::revoke\_syntax, 561

classes  
    rpki::up\_down::class\_response\_  
        syntax, 532

clear  
    rpki::async::timer, 181  
    rpki::x509::DER\_object, 581

clear\_https\_ta\_cache  
    pubd::pubd\_context, 155

rpki::left\_right::child\_elt, 304

rpki::publication::client\_elt, 366

rpki::rpki\_engine::rpkid\_context,  
    488

cli.py(3191), 638

client  
    rpki::https, 77  
    rpki::https::http\_queue, 269

client\_cert  
    rpki::https::caller, 252

client\_getopt  
    irbe\_cli::cmd\_elt\_mixin, 114

client\_handler  
    pubd::pubd\_context, 156

client\_key  
    rpki::https::caller, 252

client\_poll  
    rpki::left\_right::self\_elt, 347

client\_query\_bpki\_cert  
    irbe\_cli::cmd\_elt\_mixin, 114

client\_query\_bpki\_cms\_cert  
    irbe\_cli::cmd\_elt\_mixin, 114

client\_query\_bpki\_crl  
    irbe\_cli::config\_elt, 120

client\_query\_bpki\_https\_cert  
    irbe\_cli::cmd\_elt\_mixin, 115

client\_query\_cms\_glue  
    irbe\_cli::cmd\_elt\_mixin, 115

client\_query\_glue  
    irbe\_cli::cmd\_elt\_mixin, 115

client\_query\_https\_glue  
    irbe\_cli::cmd\_elt\_mixin, 115

client\_query\_signing\_cert  
    irbe\_cli::bsc\_elt, 105

client\_query\_signing\_cert\_crl  
    irbe\_cli::bsc\_elt, 105

client\_queues

rpkii::https, 78  
client\_reply\_decode  
    irbe\_cli::bsc\_elt, 105  
    irbe\_cli::reply\_elt\_mixin, 144  
client\_reply\_show  
    irbe\_cli::reply\_elt\_mixin, 145  
client\_ta  
    irdbd, 56  
    rootd, 64  
client\_url\_regexp  
    pubd::pubd\_context, 156  
close  
    rpkii::https::http\_stream, 284  
    rpkii::sql::session, 495  
cmd  
    rpkii::https::http\_request, 273  
cmd::Cmd, 103  
cmdloop\_with\_history  
    rpkii::cli::Cmd, 186, 188  
cms\_msg  
    irbe\_cli::left\_right\_proto, 126  
    irbe\_cli::publication\_proto, 141  
code  
    rpkii::https::http\_response, 275  
codes  
    rpkii::up\_down::error\_response\_pdu, 537  
collect\_incoming\_data  
    rpkii::https::http\_stream, 285  
columns  
    rpkii::sql::template, 507  
complete\_help  
    rpkii::cli::Cmd, 186  
completenames  
    rpkii::cli::Cmd, 187  
compose\_response  
    rootd, 62  
config.py(3107), 639  
config\_id  
    rpkii::publication::config\_elt, 372  
connect  
    rpkii::sql::session, 495  
construct\_sia\_uri  
    rpkii::rpki\_engine::ca\_obj, 462  
contains  
    rpkii::resource\_set::resource\_set, 416  
  
content  
    rpkii::x509::CMS\_object, 568  
    rpkii::x509::DER\_CMS\_object, 578  
    rpkii::x509::XML\_CMS\_object, 616  
content\_class  
    rpkii::x509::ROA, 595  
    rpkii::x509::SignedManifest, 606  
control\_handler  
    pubd::pubd\_context, 156  
convert\_to\_seconds  
    rpkii::sundial::timedelta, 518  
create  
    rpkii::rpki\_engine::ca\_detail\_obj, 453  
    rpkii::rpki\_engine::ca\_obj, 462  
    rpkii::x509::PKCS10, 591  
create\_ca  
    rpkii::x509::PKCS10, 591  
create\_top\_level  
    rpkii::xml\_utils::sax\_handler, 632  
crl\_interval  
    rpkii::left\_right::self\_elt, 352  
crl\_published  
    rpkii::rpki\_engine::ca\_detail\_obj, 457  
crl\_published\_callback  
    rpkii::rpki\_engine::ca\_detail\_obj, 453  
crl\_uri  
    rpkii::rpki\_engine::ca\_detail\_obj, 453  
crl\_uri\_tail  
    rpkii::rpki\_engine::ca\_detail\_obj, 454  
cron  
    rpkii::left\_right::self\_elt, 347  
    rpkii::rpki\_engine::rpkid\_context, 488  
cron\_keepalive  
    rpkii::rpki\_engine::rpkid\_context, 490  
cron\_period  
    rpkii::rpki\_engine::rpkid\_context, 490  
cron\_timeout

rpki::rpki\_engine::rpkid\_context, 490  
cron\_timer rpki::rpki\_engine::rpkid\_context, 490  
cronjob\_handler rpki::rpki\_engine::rpkid\_context, 488  
cross\_certify rpki::x509::X509, 608  
cur irdbd, 56  
rpki::sql::session, 497  
database rpki::sql::session, 497  
datum\_type rpki::resource\_set::resource\_range\_as, 405  
rpki::resource\_set::resource\_range\_ipv4, 411  
rpki::resource\_set::resource\_range\_ipv6, 413  
db irdbd, 56  
rpki::sql::session, 497  
debug rpki::https::caller, 253  
rpki::log, 84  
debug\_cms\_certs rpki::x509::CMS\_object, 568  
debug\_http rpki::https, 78  
debug\_tls\_certs rpki::https, 78  
decode rpki::x509::DER\_CMS\_object, 578  
rpki::x509::XML\_CMS\_object, 614  
default\_client\_timeout rpki::https, 78  
default\_http\_version rpki::https, 78  
default\_pubd\_handler rpki::left\_right::repository\_elt, 340  
default\_section rpki::config::parser, 194  
default\_server\_timeout rpki::https, 78  
defer rpki::async, 69  
deferred\_queue rpki::async, 70  
del\_subject\_cert rootd, 62  
del\_subject\_pkcs10 rootd, 62  
delete rpki::rpki\_engine::ca\_detail\_obj, 454  
rpki::rpki\_engine::ca\_obj, 462  
rpki::sql::template, 507  
DER rpki::x509::CMS\_object, 569  
rpki::x509::CRL, 574  
rpki::x509::DER\_object, 586  
rpki::x509::PKCS10, 592  
rpki::x509::RSA, 599  
rpki::x509::RSAPublic, 603  
rpki::x509::X509, 611  
description rpki::up\_down::error\_response\_pdu, 537  
detach rpki::https::http\_queue, 268  
difference rpki::resource\_set::resource\_set, 416  
dirty rpki::sql::session, 497  
do\_EOF rpki::cli::Cmd, 187  
do\_exit rpki::cli::Cmd, 187  
do\_quit rpki::cli::Cmd, 188  
doit rpki::async::iterator, 174  
done\_callback rpki::async::iterator, 174  
dump rpki::x509::DeadDrop, 576  
dump\_inbound\_cms rpki::x509::XML\_CMS\_object, 616

dump\_on\_verify\_failure  
    rpki::x509::CMS\_object, 569

dump\_outbound\_cms  
    rpki::x509::XML\_CMS\_object, 616

dump\_to\_disk  
    rpki::x509::XML\_CMS\_object, 614

dumpasn1  
    rpki::x509::DER\_object, 581

dynamic\_ta  
    rpki::https::http\_listener, 262

e  
    rpki::x509::PEM\_converter, 589

earlier  
    rpki::sundial::datetime, 511

eb  
    rpki::async::sync\_wrapper, 177

econtent\_oid  
    rpki::x509::CMS\_object, 569  
    rpki::x509::ROA, 595  
    rpki::x509::SignedManifest, 606  
    rpki::x509::XML\_CMS\_object, 616

element\_name  
    rpki::left\_right::bsc\_elt, 299  
    rpki::left\_right::child\_elt, 304  
    rpki::left\_right::list\_published\_-  
        objects\_elt, 316  
    rpki::left\_right::list\_received\_-  
        resources\_elt, 318  
    rpki::left\_right::list\_resources\_elt,  
        322  
    rpki::left\_right::list\_roa\_requests\_-  
        elt, 324  
    rpki::left\_right::parent\_elt, 333  
    rpki::left\_right::report\_error\_elt, 337  
    rpki::left\_right::repository\_elt, 341  
    rpki::left\_right::self\_elt, 352  
    rpki::publication::certificate\_elt, 362  
    rpki::publication::client\_elt, 366  
    rpki::publication::config\_elt, 373  
    rpki::publication::crl\_elt, 378  
    rpki::publication::manifest\_elt, 380  
    rpki::publication::report\_error\_elt,  
        392  
    rpki::publication::roa\_elt, 395

elements

empty  
    rpki::resource\_set::resource\_bag,  
        400  
    rpki::x509::DER\_object, 581

emptyline  
    rpki::cli::Cmd, 187

emptyline\_repeats\_last\_command  
    rpki::cli::Cmd, 188

enable\_trace  
    rpki::log, 84

encode  
    rpki::x509::DER\_CMS\_object, 578  
    rpki::x509::XML\_CMS\_object, 614

encoding  
    rpki::left\_right::cms\_msg, 307  
    rpki::publication::cms\_msg, 369  
    rpki::up\_down::cms\_msg, 534

endElement  
    rpki::left\_right::child\_elt, 303  
    rpki::publication::client\_elt, 364  
    rpki::publication::publication\_-  
        object\_elt, 386  
    rpki::up\_down::base\_elt, 521  
    rpki::up\_down::certificate\_elt, 524  
    rpki::up\_down::class\_elt, 527  
    rpki::up\_down::error\_response\_pdu,  
        536  
    rpki::up\_down::issue\_pdu, 540  
    rpki::xml\_utils::base\_elt, 618  
    rpki::xml\_utils::data\_elt, 623  
    rpki::xml\_utils::msg, 628  
    rpki::xml\_utils::sax\_handler, 632  
    rpki::xml\_utils::text\_elt, 635

endElementNS  
    rpki::xml\_utils::sax\_handler, 632

enforce\_strict\_up\_down\_xml\_sender  
    rpki::left\_right, 82

EOF\_exits\_command\_loop

rpki::cli::Cmd, 189  
err  
    rpki::async::sync\_wrapper, 178  
errback  
    rpki::async::timer, 181, 183  
    rpki::https::http\_request, 273  
error  
    rpki::log, 84  
error\_code  
    rpki::left\_right::report\_error\_elt, 337  
    rpki::publication::report\_error\_elt,  
        392  
error\_text  
    rpki::left\_right::report\_error\_elt, 337  
    rpki::publication::report\_error\_elt,  
        392  
event\_loop  
    rpki::async, 70  
Exception, 103  
exceptions  
    rpki::up\_down::error\_response\_pdu,  
        537  
exceptions.py(2907), 639  
excludes  
    irbe\_cli::bsc\_elt, 106  
    irbe\_cli::cmd\_elt\_mixin, 116  
    irbe\_cli::list\_published\_objects\_elt,  
        130  
    irbe\_cli::list\_received\_resources\_elt,  
        132  
execute  
    rpki::sql::session, 495  
executemany  
    rpki::sql::session, 496  
exit\_event\_loop  
    rpki::async, 70  
ExitNow  
    rpki::async, 70  
expect\_close  
    rpki::https::http\_client, 258  
    rpki::https::http\_server, 280  
expired  
    rpki::x509::X509, 609  
expires  
    rpki::rpk\_engine::revoked\_cert\_obj,  
        477  
explicitVersion  
    rpki::manifest::Manifest, 359  
    rpki::roa::RouteOriginAttestation,  
        449  
extract  
    rpki::x509::CMS\_object, 567  
fetch  
    rpki::publication::config\_elt, 371  
    rpki::rpk\_engine::child\_cert\_obj,  
        469  
fetch\_active  
    rpki::rpk\_engine::ca\_obj, 462  
fetch\_deprecated  
    rpki::rpk\_engine::ca\_obj, 463  
fetch\_issue\_response\_candidates  
    rpki::rpk\_engine::ca\_obj, 463  
fetch\_pending  
    rpki::rpk\_engine::ca\_obj, 463  
fetch\_revoked  
    rpki::rpk\_engine::ca\_obj, 463  
fetchall  
    rpki::sql::session, 496  
file  
    rpki::manifest::FileAndHash, 356  
fileHashAlg  
    rpki::manifest::Manifest, 359  
fileList  
    rpki::manifest::Manifest, 359  
filename  
    rpki::config::parser, 194  
filename\_complete  
    rpki::cli::Cmd, 187  
find\_handler  
    rpki::https::http\_server, 278  
format  
    rpki::https::http\_message, 264  
format\_first\_line  
    rpki::https::http\_request, 272  
    rpki::https::http\_response, 275  
formats  
    rpki::x509::CMS\_object, 569  
    rpki::x509::CRL, 574  
    rpki::x509::DER\_object, 586  
    rpki::x509::PKCS10, 592  
    rpki::x509::RSA, 599

rpkii::x509::RSAPublic, 603  
rpkii::x509::X509, 611  
found\_terminator  
    rpkii::https::http\_stream, 285  
from\_bytes  
    rpkii::ipaddrs::v4addr, 291  
    rpkii::ipaddrs::v6addr, 294  
from\_exception  
    rpkii::left\_right::report\_error\_elt, 336  
    rpkii::publication::report\_error\_elt,  
        391  
from\_resource\_bag  
    rpkii::up\_down::class\_elt, 527  
from\_rfc3779\_tuples  
    rpkii::resource\_set::resource\_bag,  
        400  
from\_sql  
    rpkii::resource\_set::resource\_set, 416  
    rpkii::resource\_set::roa\_prefix\_set,  
        437  
    rpkii::sundial::datetime, 511  
    rpkii::x509::DER\_object, 582  
fromASN1tuple  
    rpkii::sundial::datetime, 511  
fromdatetime  
    rpkii::sundial::datetime, 511  
fromGeneralizedTime  
    rpkii::sundial::datetime, 512  
fromtimedelta  
    rpkii::sundial::timedelta, 518  
fromUTCTime  
    rpkii::sundial::datetime, 512  
fromXMLtime  
    rpkii::sundial::datetime, 512  
func  
    rpkii::async::sync\_wrapper, 178  
gAKI  
    rpkii::x509::DER\_object, 582  
gc\_debug  
    rpkii::async::timer, 183  
gctx  
    rpkii::rpki\_engine::ca\_detail\_obj,  
        457  
    rpkii::rpki\_engine::ca\_obj, 465  
rpkii::rpki\_engine::child\_cert\_obj,  
    470  
rpkii::rpki\_engine::revoked\_cert\_obj,  
    477  
rpkii::rpki\_engine::roa\_obj, 484  
rpkii::sql::sql\_persistent, 504  
generate  
    rpkii::rpki\_engine::roa\_obj, 481  
    rpkii::x509::CRL, 572  
    rpkii::x509::RSA, 598  
generate\_crl  
    rpkii::rpki\_engine::ca\_detail\_obj,  
        454  
generate\_manifest  
    rpkii::rpki\_engine::ca\_detail\_obj,  
        454  
generate\_manifest\_cert  
    rpkii::rpki\_engine::ca\_detail\_obj,  
        454  
get  
    rpkii::config::parser, 192  
get\_3779resources  
    rpkii::x509::DER\_object, 582  
get\_AIA  
    rpkii::x509::DER\_object, 582  
get\_aia\_uri  
    rpkii::x509::DER\_object, 582  
get\_AKI  
    rpkii::x509::DER\_object, 583  
get\_Base64  
    rpkii::x509::DER\_object, 583  
get\_basicConstraints  
    rpkii::x509::DER\_object, 583  
get\_buffer  
    rpkii::https::http\_stream, 285  
get\_content  
    rpkii::x509::CMS\_object, 567  
get\_DER  
    rpkii::x509::CMS\_object, 567  
    rpkii::x509::CRL, 572  
    rpkii::x509::DER\_object, 583  
    rpkii::x509::PKCS10, 592  
    rpkii::x509::RSA, 598  
    rpkii::x509::RSAPublic, 602  
    rpkii::x509::X509, 609  
get\_PEM

rpkii::x509::DER\_object, 583  
get\_POW  
    rpkii::x509::CMS\_object, 567  
    rpkii::x509::CRL, 573  
    rpkii::x509::RSA, 598  
    rpkii::x509::RSApublic, 602  
    rpkii::x509::X509, 609  
get\_POWpkix  
    rpkii::x509::CRL, 573  
    rpkii::x509::PKCS10, 592  
    rpkii::x509::X509, 609  
get\_public\_DER  
    rpkii::x509::RSA, 599  
get\_root\_cert  
    rootd, 62  
get\_RSApublic  
    rpkii::x509::RSA, 599  
get\_SIA  
    rpkii::x509::DER\_object, 584  
get\_sia\_directory\_uri  
    rpkii::x509::DER\_object, 584  
get\_sia\_manifest\_uri  
    rpkii::x509::DER\_object, 584  
get\_SKI  
    rpkii::up\_down::revoke\_pdu, 557  
    rpkii::x509::DER\_object, 584  
    rpkii::x509::RSA, 599  
    rpkii::x509::RSApublic, 602  
get\_subject\_cert  
    rootd, 63  
get\_subject\_pkcs10  
    rootd, 63  
getboolean  
    rpkii::config::parser, 192  
getint  
    rpkii::config::parser, 192  
getIssuer  
    rpkii::x509::CRL, 573  
    rpkii::x509::X509, 609  
getlong  
    rpkii::config::parser, 192  
getNextUpdate  
    rpkii::x509::CRL, 573  
    rpkii::x509::SignedManifest, 605  
getNotAfter  
    rpkii::x509::X509, 609  
getNotBefore  
    rpkii::x509::X509, 610  
getPublicKey  
    rpkii::x509::PKCS10, 592  
    rpkii::x509::X509, 610  
getSerial  
    rpkii::x509::X509, 610  
getSubject  
    rpkii::x509::X509, 610  
getThisUpdate  
    rpkii::x509::CRL, 573  
    rpkii::x509::SignedManifest, 605  
gSKI  
    rpkii::x509::DER\_object, 584  
hAKI  
    rpkii::x509::DER\_object, 585  
handle\_accept  
    rpkii::https::http\_listener, 261  
handle\_body  
    rpkii::https::http\_stream, 285  
handle\_close  
    rpkii::https::http\_client, 255  
    rpkii::https::http\_stream, 286  
handle\_connect  
    rpkii::https::http\_client, 256  
handle\_dispatch  
    irdbd, 57  
handle\_error  
    rpkii::https::http\_client, 256  
    rpkii::https::http\_listener, 261  
    rpkii::https::http\_stream, 286  
handle\_list\_resources  
    irdbd, 55  
handle\_list\_roa\_requests  
    irdbd, 55  
handle\_message  
    rpkii::https::http\_client, 256  
    rpkii::https::http\_server, 278  
handle\_no\_content\_length  
    rpkii::https::http\_client, 256  
    rpkii::https::http\_server, 279  
handle\_read  
    rpkii::https::http\_stream, 286  
handle\_timeout  
    rpkii::https::http\_client, 257

rpkii::https::http\_stream, 286  
handle\_write  
    rpkii::https::http\_stream, 287  
handler  
    irdbd, 56  
        rpkii::async::gc\_summary, 171  
        rpkii::async::timer, 182, 184  
    handler\_common  
        pubd::pubd\_context, 156  
handlers  
    irdbd, 57  
    rootd, 64  
        rpkii::https::http\_listener, 262  
        rpkii::https::http\_server, 280  
        rpkii::rpki\_engine::publication\_queue, 474  
handles  
    rpkii::left\_right::bsc\_elt, 299  
    rpkii::left\_right::child\_elt, 305  
    rpkii::left\_right::data\_elt, 311  
    rpkii::left\_right::parent\_elt, 333  
    rpkii::left\_right::repository\_elt, 342  
    rpkii::left\_right::self\_elt, 352  
has\_option  
    rpkii::config::parser, 192  
has\_section  
    rpkii::config::parser, 193  
hash  
    rpkii::manifest::FileAndHash, 356  
have\_readline  
    rpkii::cli, 72  
headers  
    rpkii::https::http\_message, 266  
help\_help  
    rpkii::cli::Cmd, 188  
histfile  
    rpkii::cli::Cmd, 189  
host  
    irdbd, 57  
    rootd, 64  
hostport  
    rpkii::https::http\_client, 258  
    rpkii::https::http\_queue, 270  
hSKI  
    rpkii::x509::DER\_object, 585  
https.py(3191), 641  
  
https\_server\_host  
    pubd::pubd\_context, 157  
    rootd, 65  
    rpkii::rpki\_engine::rpkid\_context, 491  
https\_server\_port  
    pubd::pubd\_context, 157  
    rootd, 65  
    rpkii::rpki\_engine::rpkid\_context, 491  
https\_ta\_cache  
    pubd::pubd\_context, 157  
    rpkii::rpki\_engine::rpkid\_context, 491  
identchars  
    rpkii::cli::Cmd, 189  
index  
    rpkii::sql::template, 507  
info  
    rpkii::log, 84  
inherit  
    rpkii::resource\_set::resource\_set, 417  
    rpkii::resource\_set::resource\_set\_as, 420  
    rpkii::resource\_set::resource\_set\_ip, 423  
inherit\_token  
    rpkii::resource\_set, 92  
init  
    rpkii::log, 83  
initial\_delay  
    rpkii::rpki\_engine::rpkid\_context, 491  
initiate\_send  
    rpkii::https::http\_stream, 287  
insert  
    rpkii::sql::template, 507  
intersection  
    rpkii::resource\_set::resource\_bag, 400  
    rpkii::resource\_set::resource\_set, 416  
interval  
    rpkii::async::gc\_summary, 171  
ipAddrBlocks

rpki::roa::RouteOriginAttestation, 449  
ipaddrs.py(2424), 642  
ipv4  
    rpki::left\_right::list\_resources\_elt, 322  
    rpki::left\_right::list\_roa\_requests\_elt, 325  
    rpki::rpki\_engine::roa\_obj, 484  
ipv6  
    rpki::left\_right::list\_resources\_elt, 322  
    rpki::left\_right::list\_roa\_requests\_elt, 325  
    rpki::rpki\_engine::roa\_obj, 484  
irbe\_cert  
    pubd::pubd\_context, 157  
    rpki::rpki\_engine::rpkid\_context, 491  
irbe\_cli, 50  
    argv, 52  
    call\_pubd, 52  
    call\_rpkid, 52  
    cfg, 52  
    cfg\_file, 53  
    pem\_out, 53  
    q\_msg, 53  
    q\_msg\_left\_right, 53  
    q\_msg\_publication, 53  
    q\_pdu, 53  
    top\_opts, 53  
    usage, 52  
    usage\_fill, 54  
    verbose, 54  
irbe\_cli.py(3107), 642  
irbe\_cli::bsc\_elt, 103  
    client\_query\_signing\_cert, 105  
    client\_query\_signing\_cert\_crl, 105  
    client\_reply\_decode, 105  
    excludes, 106  
    signing\_cert, 106  
    signing\_cert\_crl, 106  
irbe\_cli::certificate\_elt, 106  
irbe\_cli::child\_elt, 108  
irbe\_cli::client\_elt, 110  
irbe\_cli::cmd\_elt\_mixin, 112  
bpki\_cert, 116  
bpki\_cms\_cert, 116  
bpki\_cms\_glue, 116  
bpki\_glue, 116  
bpki\_https\_cert, 116  
bpki\_https\_glue, 116  
client\_getopt, 114  
client\_query\_bpki\_cert, 114  
client\_query\_bpki\_cms\_cert, 114  
client\_query\_bpki\_https\_cert, 115  
client\_query\_cms\_glue, 115  
client\_query\_glue, 115  
client\_query\_https\_glue, 115  
excludes, 116  
is\_cmd, 117  
usage, 115  
irbe\_cli::cmd\_msg\_mixin, 117  
usage, 118  
irbe\_cli::config\_elt, 118  
    bpki\_crl, 120  
    client\_query\_bpki\_crl, 120  
irbe\_cli::crl\_elt, 120  
irbe\_cli::left\_right\_cms\_msg, 122  
    saxify, 123  
irbe\_cli::left\_right\_msg, 123  
    pdus, 125  
irbe\_cli::left\_right\_proto, 125  
    cms\_msg, 126  
    msg, 126  
irbe\_cli::left\_right\_sax\_handler, 127  
    pdu, 128  
irbe\_cli::list\_published\_objects\_elt, 128  
    excludes, 130  
irbe\_cli::list\_received\_resources\_elt, 130  
    excludes, 132  
irbe\_cli::manifest\_elt, 132  
irbe\_cli::parent\_elt, 134  
irbe\_cli::publication\_cms\_msg, 136  
    saxify, 138  
irbe\_cli::publication\_msg, 138  
    pdus, 140  
irbe\_cli::publication\_proto, 140  
    cms\_msg, 141  
    msg, 141  
irbe\_cli::publication\_sax\_handler, 142  
    pdu, 143

irbe\_cli::reply\_elt\_mixin, 143  
    client\_reply\_decode, 144  
    client\_reply\_show, 145  
    is\_cmd, 145  
irbe\_cli::report\_error\_elt, 145  
irbe\_cli::repository\_elt, 146  
irbe\_cli::roa\_elt, 148  
irbe\_cli::self\_elt, 150  
irbe\_cli::UsageWrapper, 152  
    \_\_call\_\_, 153  
irdb\_cert  
    rpki::rpki\_engine::rpkid\_context,  
        491  
irdb\_query  
    rpki::rpki\_engine::rpkid\_context,  
        489  
irdb\_query\_child\_resources  
    rpki::rpki\_engine::rpkid\_context,  
        489  
irdb\_query\_roa\_requests  
    rpki::rpki\_engine::rpkid\_context,  
        489  
irdb\_url  
    rpki::rpki\_engine::rpkid\_context,  
        491  
irdbd, 54  
    bpki\_ta, 56  
    cfg, 56  
    cfg\_file, 56  
    client\_ta, 56  
    cur, 56  
    db, 56  
    handle\_dispatch, 57  
    handle\_list\_resources, 55  
    handle\_list\_roa\_requests, 55  
    handler, 56  
    handlers, 57  
    host, 57  
    irdbd\_cert, 57  
    irdbd\_key, 57  
    port, 57  
    rpkid\_cert, 58  
    server\_cert, 58  
    startup\_msg, 58  
    u, 58  
irdbd.py(2913), 644  
irdbd\_cert  
    irdbd, 57  
irdbd\_key  
    irdbd, 57  
is\_CA  
    rpki::x509::DER\_object, 585  
is\_cmd  
    irbe\_cli::cmd\_elt\_mixin, 117  
    irbe\_cli::reply\_elt\_mixin, 145  
is\_query  
    rpki::xml\_utils::msg, 628  
is\_reply  
    rpki::xml\_utils::msg, 628  
is\_set  
    rpki::async::timer, 182  
issubset  
    rpki::resource\_set::resource\_set, 416  
issue  
    rpki::rpki\_engine::ca\_detail\_obj,  
        455  
    rpki::x509::X509, 610  
issue\_ee  
    rpki::rpki\_engine::ca\_detail\_obj,  
        455  
issue\_subject\_cert\_maybe  
    rootd, 63  
issuer  
    rpki::up\_down::class\_elt, 529  
issuperset  
    rpki::resource\_set::resource\_set, 417  
item\_callback  
    rpki::async::iterator, 174  
iterator  
    rpki::async::iterator, 174  
key  
    rpki::https::http\_client, 258  
    rpki::https::http\_listener, 262  
    rpki::https::http\_queue, 270  
last\_crl\_sn  
    rpki::rpki\_engine::ca\_obj, 465  
last\_issued\_sn  
    rpki::rpki\_engine::ca\_obj, 465  
last\_manifest\_sn  
    rpki::rpki\_engine::ca\_obj, 465

lastrowid  
    rpki::sql::session, 496

later  
    rpki::sundial::datetime, 512

latest\_ca\_cert  
    rpki::rpki\_engine::ca\_detail\_obj,  
        457

latest\_crl  
    rpki::rpki\_engine::ca\_detail\_obj,  
        457

latest\_manifest  
    rpki::rpki\_engine::ca\_detail\_obj,  
        458

latest\_manifest\_cert  
    rpki::rpki\_engine::ca\_detail\_obj,  
        458

left\_right  
    rpki::relaxng, 89

left\_right.py(3191), 644

left\_right\_handler  
    rpki::rpki\_engine::rpkid\_context,  
        489

log  
    rpki::https::http\_listener, 262  
    rpki::https::http\_queue, 270  
    rpki::https::http\_stream, 289

log.py(3107), 645

log\_cert  
    rpki::https::http\_stream, 287

log\_method  
    rpki::https, 77

log\_query  
    root::message\_pdu, 166  
    rpki::up\_down::message\_pdu, 550

long, 153

looks\_like\_PEM  
    rpki::x509::PEM\_converter, 588

maildir  
    rpki::x509::DeadDrop, 576

main  
    pubd, 59  
    rpkid, 102

make\_b64elt  
    rpki::up\_down::base\_elt, 521  
    rpki::xml\_utils::base\_elt, 619

make\_elt  
    rpki::up\_down::base\_elt, 521  
    rpki::xml\_utils::base\_elt, 619

make\_pdu  
    rpki::xml\_utils::base\_elt, 619

make\_prefix  
    rpki::resource\_set::resource\_range\_-  
        ip, 408

make\_publish  
    rpki::publication::publication\_-  
        object\_elt, 386

make\_query  
    rpki::up\_down::message\_pdu, 550

make\_reply  
    rpki::left\_right::list\_published\_-  
        objects\_elt, 315  
    rpki::left\_right::list\_received\_-  
        resources\_elt, 318  
    rpki::xml\_utils::data\_elt, 623

make\_reply\_clone\_hook  
    rpki::left\_right::data\_elt, 309  
    rpki::xml\_utils::data\_elt, 623

make\_withdraw  
    rpki::publication::publication\_-  
        object\_elt, 387

manifest.py(2424), 646

manifest\_private\_key\_id  
    rpki::rpki\_engine::ca\_detail\_obj,  
        458

manifest\_public\_key  
    rpki::rpki\_engine::ca\_detail\_obj,  
        458

manifest\_published  
    rpki::rpki\_engine::ca\_detail\_obj,  
        458

manifest\_published\_callback  
    rpki::rpki\_engine::ca\_detail\_obj,  
        455

manifest\_uri  
    rpki::rpki\_engine::ca\_detail\_obj,  
        455

manifestNumber  
    rpki::manifest::Manifest, 359

map  
    rpki::sql::template, 508

max

rpki::resource\_set::resource\_range, 403  
rpki::resource\_set::roa\_prefix, 429  
max\_prefixlen  
    rpki::resource\_set::roa\_prefix, 430  
maxLength  
    rpki::roa::ROAIPAddress, 444  
min  
    rpki::resource\_set::resource\_range, 403  
        rpki::resource\_set::resource\_range\_as, 406  
    rpki::resource\_set::roa\_prefix, 430  
msg  
    irbe\_cli::left\_right\_proto, 126  
    irbe\_cli::publication\_proto, 141  
    rpki::https::http\_stream, 289  
msgs  
    rpki::rpki\_engine::publication\_queue, 474  
multiget  
    rpki::config::parser, 193  
name  
    rpki::left\_right::sax\_handler, 344  
    rpki::publication::sax\_handler, 397  
    rpki::up\_down::sax\_handler, 564  
name2oid  
    rpki::oids, 87  
name2type  
    root::message\_pdu, 166  
    rpki::up\_down::message\_pdu, 552  
next\_crl\_number  
    rpki::rpki\_engine::ca\_obj, 463  
next\_manifest\_number  
    rpki::rpki\_engine::ca\_obj, 464  
next\_serial\_number  
    rpki::rpki\_engine::ca\_obj, 464  
nextUpdate  
    rpki::manifest::Manifest, 359  
    rpki::rpki\_engine::ca\_detail\_obj, 458  
normalize\_chain  
    rpki::x509::X509, 611  
normalize\_headers  
    rpki::https::http\_message, 265  
note  
    rpki::log, 85  
now  
    rpki::sundial, 96  
nsmap  
    rpki::left\_right::left\_right\_namespace, 312  
    rpki::publication::publication\_namespace, 384  
    rpki::up\_down, 98  
obj  
    rpki::left\_right::list\_published\_objects\_elt, 316  
object, 153  
oid2name  
    rpki::oids, 87  
oids.py(2424), 646  
onecmd  
    rpki::cli::Cmd, 188  
other\_clear  
    rpki::x509::CMS\_object, 569  
    rpki::x509::DER\_object, 586  
oversized  
    rpki::resource\_set::resource\_bag, 400  
parent  
    rpki::rpki\_engine::ca\_obj, 464  
parent\_id  
    rpki::rpki\_engine::ca\_obj, 465  
parent\_resource\_class  
    rpki::rpki\_engine::ca\_obj, 465  
parents  
    rpki::left\_right::bsc\_elt, 297  
    rpki::left\_right::child\_elt, 303  
    rpki::left\_right::repository\_elt, 341  
    rpki::left\_right::self\_elt, 347  
parse  
    rpki::sundial::timedelta, 519  
parse\_first\_line  
    rpki::https::http\_request, 272  
    rpki::https::http\_response, 275  
parse\_from\_wire  
    rpki::https::http\_message, 265  
parse\_rfc3779\_tuple

rpkii::resource\_set::resource\_set\_as,  
    419  
rpkii::resource\_set::resource\_set\_ip,  
    422  
parse\_str  
    rpkii::resource\_set::resource\_set\_as,  
        419  
    rpkii::resource\_set::resource\_set\_ip,  
        422  
    rpkii::resource\_set::roa\_prefix\_set,  
        437  
parse\_type  
    rpkii::https::http\_client, 258  
    rpkii::https::http\_server, 280  
parse\_version  
    rpkii::https::http\_message, 265  
password  
    rpkii::sql::session, 497  
path  
    rpkii::https::http\_request, 273  
payload  
    rpkii::publication::publication\_-  
        object\_elt, 388  
    rpkii::up\_down::message\_pdu, 552  
payload\_type  
    rpkii::publication::certificate\_elt, 362  
    rpkii::publication::crl\_elt, 378  
    rpkii::publication::manifest\_elt, 380  
    rpkii::publication::publication\_-  
        object\_elt, 388  
    rpkii::publication::roa\_elt, 395  
pdu  
    irbe\_cli::left\_right\_sax\_handler, 128  
    irbe\_cli::publication\_sax\_handler,  
        143  
    rootd::sax\_handler, 170  
    rpkii::left\_right::sax\_handler, 344  
    rpkii::publication::sax\_handler, 397  
    rpkii::up\_down::sax\_handler, 564  
pdus  
    irbe\_cli::left\_right\_msg, 125  
    irbe\_cli::publication\_msg, 140  
    rpkii::left\_right::msg, 327  
    rpkii::publication::msg, 382  
pem\_converter  
    rpkii::x509::CMS\_object, 570  
rpkii::x509::CRL, 574  
rpkii::x509::DER\_object, 586  
rpkii::x509::PKCS10, 593  
rpkii::x509::ROA, 595  
rpkii::x509::RSA, 600  
rpkii::x509::RSAPublic, 603  
rpkii::x509::SignedManifest, 606  
rpkii::x509::X509, 611  
pem\_out  
    irbe\_cli, 53  
persistent  
    rpkii::https::http\_message, 265  
pid  
    rpkii::log, 85  
    rpkii::x509::DeadDrop, 576  
ping  
    rpkii::sql::session, 496  
pkcs10  
    rpkii::up\_down::issue\_pdu, 541  
pkcs10\_request  
    rpkii::left\_right::bsc\_elt, 299  
PKIX\_threshhold  
    rpkii::sundial::datetime, 514  
port  
    irdbd, 57  
    rootd, 65  
POW  
    rpkii::x509::CMS\_object, 570  
    rpkii::x509::CRL, 574  
    rpkii::x509::RSA, 600  
    rpkii::x509::RSAPublic, 603  
    rpkii::x509::X509, 612  
POWify\_OID  
    rpkii::x509, 100  
POWpkix  
    rpkii::x509::CRL, 574  
    rpkii::x509::PKCS10, 593  
    rpkii::x509::X509, 612  
prefix  
    rpkii::resource\_set::roa\_prefix, 430  
prefix\_type  
    rpkii::resource\_set::roa\_prefix\_set\_-  
        ipv4, 440  
    rpkii::resource\_set::roa\_prefix\_set\_-  
        ipv6, 442  
prefixlen

rpkii::resource\_set::roa\_prefix, 431  
pretty\_print\_content  
    rpki::x509::XML\_CMS\_object, 615  
print\_on\_der\_error  
    rpki::x509::CMS\_object, 570  
priority  
    rpki::log::logger, 354  
private\_key\_id  
    rpki::left\_right::bsc\_elt, 299  
    rpki::rpki\_engine::ca\_detail\_obj,  
        458  
profile  
    pubd, 60  
    rpkid, 102  
proto  
    rpki::https::caller, 253  
pubd, 58  
    cfg\_file, 60  
    main, 59  
    profile, 60  
pubd.py(3107), 647  
pubd::pubd\_context, 153  
    \_\_init\_\_, 155  
    bpki\_ta, 156  
    build\_https\_ta\_cache, 155  
    clear\_https\_ta\_cache, 155  
    client\_handler, 156  
    client\_url\_regexp, 156  
    control\_handler, 156  
    handler\_common, 156  
    https\_server\_host, 157  
    https\_server\_port, 157  
    https\_ta\_cache, 157  
    irbe\_cert, 157  
    pubd\_cert, 157  
    pubd\_key, 157  
    publication\_base, 157  
    publication\_multimodule, 158  
    sql, 158  
pubd\_cert  
    pubd::pubd\_context, 157  
pubd\_key  
    pubd::pubd\_context, 157  
public\_key  
    rpki::rpki\_engine::ca\_detail\_obj,  
        459  
publication  
    rpki::relaxng, 89  
publication.py(3107), 647  
publication\_base  
    pubd::pubd\_context, 157  
publication\_kludge\_base  
    rpki::rpki\_engine::rpkid\_context,  
        492  
publication\_multimodule  
    pubd::pubd\_context, 158  
publish  
    rpki::rpki\_engine::publication\_-  
        queue, 473  
published  
    rpki::rpki\_engine::child\_cert\_obj,  
        470  
    rpki::rpki\_engine::roa\_obj, 484  
published\_callback  
    rpki::rpki\_engine::child\_cert\_obj,  
        469  
    rpki::rpki\_engine::roa\_obj, 481  
pydatetime::datetime, 158  
pydatetime::timedelta, 158  
  
q\_msg  
    irbe\_cli, 53  
q\_msg\_left\_right  
    irbe\_cli, 53  
q\_msg\_publication  
    irbe\_cli, 53  
q\_pdu  
    irbe\_cli, 53  
query  
    rpki::up\_down::issue\_pdu, 540  
    rpki::up\_down::list\_pdu, 546  
    rpki::up\_down::revoke\_pdu, 557  
    rpki::xml\_utils::msg, 628  
query\_up\_down  
    rpki::left\_right::parent\_elt, 330  
queue  
    rpki::async::timer, 184  
    rpki::https::http\_client, 259  
    rpki::https::http\_queue, 270  
raise\_if\_error

rpki::publication::publication\_object\_elt, 387  
rpki::publication::report\_error\_elt, 392  
range\_type  
    rpki::resource\_set::resource\_set\_as, 420  
    rpki::resource\_set::resource\_set\_ipv4, 425  
    rpki::resource\_set::resource\_set\_ipv6, 427  
    rpki::resource\_set::roa\_prefix\_ipv4, 433  
    rpki::resource\_set::roa\_prefix\_ipv6, 435  
readAttrs  
    rpki::xml\_utils::base\_elt, 619  
readable  
    rpki::https::http\_stream, 287  
reason  
    rpki::https::http\_response, 275  
recipient  
    rpki::up\_down::message\_pdu, 552  
recv  
    rpki::https::http\_stream, 287  
regen\_margin  
    rpki::left\_right::self\_elt, 352  
regenerate  
    rpki::rpki\_engine::roa\_obj, 481  
regenerate\_crls\_and\_manifests  
    rpki::left\_right::self\_elt, 348  
regexp  
    rpki::sundial::timedelta, 519  
reissue  
    rpki::rpki\_engine::child\_cert\_obj, 469  
rekey  
    rpki::rpki\_engine::ca\_obj, 464  
relaxng.py(3110), 648  
replace  
    rpki::rpki\_engine::publication\_queue, 474  
reply  
    rpki::xml\_utils::msg, 629  
repositories  
    rpki::left\_right::bsc\_elt, 298  
rpki::left\_right::self\_elt, 348  
rpki::rpki\_engine::publication\_queue, 474  
repository  
    rpki::left\_right::parent\_elt, 331  
req\_resource\_set\_as  
    rpki::up\_down::certificate\_elt, 525  
    rpki::up\_down::issue\_pdu, 541  
req\_resource\_set\_ipv4  
    rpki::up\_down::certificate\_elt, 525  
    rpki::up\_down::issue\_pdu, 541  
req\_resource\_set\_ipv6  
    rpki::up\_down::certificate\_elt, 525  
    rpki::up\_down::issue\_pdu, 541  
request  
    rpki::https::http\_queue, 268  
require\_crls  
    rpki::x509::CMS\_object, 570  
res  
    rpki::async::sync\_wrapper, 178  
resource\_set.py(3107), 648  
resource\_set\_as  
    rpki::up\_down::class\_elt, 529  
resource\_set\_ipv4  
    rpki::up\_down::class\_elt, 529  
resource\_set\_ipv6  
    rpki::up\_down::class\_elt, 529  
resource\_set\_notafter  
    rpki::up\_down::class\_elt, 529  
resource\_set\_type  
    rpki::resource\_set::roa\_prefix\_set\_ipv4, 440  
    rpki::resource\_set::roa\_prefix\_set\_ipv6, 442  
restart  
    rpki::https::http\_queue, 269  
    rpki::https::http\_stream, 288  
result  
    rpki::xml\_utils::sax\_handler, 633  
retry  
    rpki::https::http\_request, 273  
retry\_read  
    rpki::https::http\_client, 259  
    rpki::https::http\_server, 280  
    rpki::https::http\_stream, 289  
retry\_write

rpkii::https::http\_client, 259  
rpkii::https::http\_server, 280  
rpkii::https::http\_stream, 289  
return\_result  
    rpkii::https::http\_queue, 269  
revoke  
    rpkii::rpki\_engine::ca\_detail\_obj,  
        455  
    rpkii::rpki\_engine::ca\_obj, 464  
    rpkii::rpki\_engine::child\_cert\_obj,  
        469  
    rpkii::rpki\_engine::revoked\_cert\_obj,  
        476  
    rpkii::rpki\_engine::roa\_obj, 481  
revoked  
    rpkii::rpki\_engine::revoked\_cert\_obj,  
        477  
revoked\_certs  
    rpkii::rpki\_engine::ca\_detail\_obj,  
        456  
roa  
    rpkii::rpki\_engine::roa\_obj, 484  
roa.py(2424), 649  
roas  
    rpkii::left\_right::self\_elt, 348  
    rpkii::rpki\_engine::ca\_detail\_obj,  
        456  
root\_newer\_than\_subject  
    rootd, 63  
rootd, 60  
    bpki\_ta, 64  
    cfg, 64  
    cfg\_file, 64  
    child\_bpki\_cert, 64  
    client\_ta, 64  
    compose\_response, 62  
    del\_subject\_cert, 62  
    del\_subject\_pkcs10, 62  
    get\_root\_cert, 62  
    get\_subject\_cert, 63  
    get\_subject\_pkcs10, 63  
    handlers, 64  
    host, 64  
    https\_server\_host, 65  
    https\_server\_port, 65  
    issue\_subject\_cert\_maybe, 63  
port, 65  
root\_newer\_than\_subject, 63  
rootd\_bpki\_cert, 65  
rootd\_bpki\_crl, 65  
rootd\_bpki\_key, 65  
rpki\_base\_uri, 65  
rpki\_class\_name, 66  
rpki\_root\_cert, 66  
rpki\_root\_cert\_file, 66  
rpki\_root\_cert\_uri, 66  
rpki\_root\_crl, 66  
rpki\_root\_dir, 66  
rpki\_root\_key, 66  
rpki\_root\_manifest, 67  
rpki\_subject\_cert, 67  
rpki\_subject\_lifetime, 67  
rpki\_subject\_pkcs10, 67  
rpki\_subject\_regen, 67  
server\_cert, 67  
set\_subject\_cert, 63  
set\_subject\_pkcs10, 63  
up\_down\_handler, 63  
rootd.py(2913), 649  
rootd::cms\_msg, 158  
    saxify, 160  
rootd::issue\_pdu, 160  
    serve\_pdu, 162  
rootd::list\_pdu, 162  
    serve\_pdu, 164  
rootd::message\_pdu, 164  
    log\_query, 166  
    name2type, 166  
    type2name, 166  
rootd::revoke\_pdu, 167  
    serve\_pdu, 168  
rootd::sax\_handler, 168  
    pdu, 170  
rootd\_bpki\_cert  
    rootd, 65  
rootd\_bpki\_crl  
    rootd, 65  
rootd\_bpki\_key  
    rootd, 65  
rpki, 68  
rpki.\_\_doc\_\_, 68  
rpki.async, 68

rpki.cli, 71  
rpki.config, 72  
rpki.exceptions, 73  
rpki.https, 75  
rpki.ipaddrs, 80  
rpki.left\_right, 81  
rpki.log, 82  
rpki.manifest, 85  
rpki.oids, 86  
rpki.publication, 88  
rpki.relaxng, 89  
rpki.resource\_set, 89  
rpki.roa, 92  
rpki.rpki\_engine, 93  
rpki.sql, 94  
rpki.sundial, 95  
rpki.up\_down, 97  
rpki.x509, 98  
rpki.xml\_utils, 100  
rpki::async  
    \_raiseExitNow, 69  
    defer, 69  
    deferred\_queue, 70  
    event\_loop, 70  
    exit\_event\_loop, 70  
    ExitNow, 70  
    run\_deferred, 70  
rpki::async::gc\_summary, 170  
    \_\_init\_\_, 171  
    handler, 171  
    interval, 171  
    threshold, 171  
    timer, 171  
rpki::async::iterator, 172  
    \_\_call\_\_, 173  
    \_\_init\_\_, 173  
    \_\_repr\_\_, 174  
    caller\_function, 174  
    doit, 174  
    done\_callback, 174  
    item\_callback, 174  
    iterator, 174  
    unwind\_stack, 175  
rpki::async::sync\_wrapper, 175  
    \_\_call\_\_, 177  
    \_\_init\_\_, 177  
        cb, 177  
        eb, 177  
        err, 178  
        func, 178  
        res, 178  
    rpki::async::timer, 178  
        \_\_cmp\_\_, 181  
        \_\_del\_\_, 181  
        \_\_init\_\_, 181  
        \_\_repr\_\_, 181  
        cancel, 181  
        clear, 181  
        errback, 181, 183  
        gc\_debug, 183  
        handler, 182, 184  
        is\_set, 182  
        queue, 184  
        run\_debug, 184  
        runq, 182  
        seconds\_until\_wakeup, 182  
        set, 182  
        set\_errback, 183  
        set\_handler, 183  
        trace, 183  
        when, 184  
rpki::cli  
    \_\_yes\_or\_no\_prompts, 72  
    have\_readline, 72  
    yes\_or\_no, 71  
rpki::cli::Cmd, 184  
    \_\_init\_\_, 186  
    cmdloop\_with\_history, 186, 188  
    complete\_help, 186  
    completename, 187  
    do\_EOF, 187  
    do\_exit, 187  
    do\_quit, 188  
    emptyline, 187  
    emptyline\_repeats\_last\_command,  
        188  
    EOF\_exits\_command\_loop, 189  
    filename\_complete, 187  
    help\_help, 188  
    histfile, 189  
    identchars, 189  
    onecmd, 188

rpk::config::parser, 189  
    \_\_init\_\_, 191  
    \_reEXP, 193  
    \_repl, 191  
    cfg, 193  
    default\_section, 194  
    filename, 194  
    get, 192  
    getboolean, 192  
    getint, 192  
    getlong, 192  
    has\_option, 192  
    has\_section, 193  
    multiget, 193  
        set\_global\_flags, 193  
rpk::exceptions::BadClassNameSyntax, 194  
rpk::exceptions::BadClientURL, 195  
rpk::exceptions::BadContactURL, 196  
rpk::exceptions::BadExtension, 197  
rpk::exceptions::BadIRDBReply, 198  
rpk::exceptions::BadIssueResponse, 199  
rpk::exceptions::BadPKCS10, 200  
rpk::exceptions::BadPublicationReply, 201  
rpk::exceptions::BadQuery, 202  
rpk::exceptions::BadSender, 203  
rpk::exceptions::BadStatusCode, 204  
rpk::exceptions::BadURISyntax, 205  
rpk::exceptions::BSCNotFound, 206  
rpk::exceptions::BSCNotReady, 207  
rpk::exceptions::ChildNotFound, 208  
rpk::exceptions::ClassNameMismatch, 209  
rpk::exceptions::ClassNameUnknown, 210  
rpk::exceptions::ClientNotFound, 211  
rpk::exceptions::CMSContentNotSet, 212  
rpk::exceptions::CMSCRLNotSet, 214  
rpk::exceptions::CMSVerificationFailed, 215  
rpk::exceptions::DBConsistencyError, 216  
rpk::exceptions::DERObjectConversionError, 217  
rpk::exceptions::DuplicateObject, 218  
rpk::exceptions::EmptyPEM, 219  
rpk::exceptions::EmptyROAPrefixList, 220  
rpk::exceptions::ForbiddenURI, 221  
rpk::exceptions::HandleTranslationError, 222  
rpk::exceptions::HTTPRequestFailed, 223  
rpk::exceptions::HTTPPSBadVersion, 224  
rpk::exceptions::HTTPPSClientAborted, 225  
rpk::exceptions::HTTPSUnexpectedState, 226  
rpk::exceptions::MissingCMSCRL, 227  
rpk::exceptions::MissingCMSEcert, 228  
rpk::exceptions::MultipleTLSEECert, 229  
rpk::exceptions::MustBePrefix, 230  
rpk::exceptions::NoActiveCA, 231  
rpk::exceptions::NoCoveringCertForROA, 232  
rpk::exceptions::NoObjectAtURI, 233  
rpk::exceptions::NotACertificateChain, 234  
rpk::exceptions::NotFound, 235  
rpk::exceptions::NotImplementedYet, 236  
rpk::exceptions::NotInDatabase, 237  
rpk::exceptions::ReceivedTLSACert, 238  
rpk::exceptions::RPKI\_Exception, 240  
rpk::exceptions::ServerShuttingDown, 241  
rpk::exceptions::SKIMismatch, 242  
rpk::exceptions::SubprocessError, 243  
rpk::exceptions::TLSValidation, 244  
rpk::exceptions::UnexpectedCMSCerts, 246  
rpk::exceptions::UnexpectedCMSCRLs, 247  
rpk::exceptions::UnparsableCMSDER, 248  
rpk::exceptions::UpstreamError, 249

rpki::exceptions::WrongEContentType, 250  
rpki::https  
    build\_https\_ta\_cache, 77  
    client, 77  
    client\_queues, 78  
    debug\_http, 78  
    debug\_tls\_certs, 78  
    default\_client\_timeout, 78  
    default\_http\_version, 78  
    default\_server\_timeout, 78  
    log\_method, 77  
    rpki\_content\_type, 79  
    server, 77  
    supported\_address\_families, 79  
    want\_persistent\_client, 79  
    want\_persistent\_server, 79  
rpki::https::caller, 251  
    \_\_call\_\_, 252  
    \_\_init\_\_, 252  
    client\_cert, 252  
    client\_key, 252  
    debug, 253  
    proto, 253  
    server\_cert, 253  
    server\_ta, 253  
    url, 253  
rpki::https::http\_client, 253  
    \_\_init\_\_, 255  
    af, 258  
    cert, 258  
    expect\_close, 258  
    handle\_close, 255  
    handle\_connect, 256  
    handle\_error, 256  
    handle\_message, 256  
    handle\_no\_content\_length, 256  
    handle\_timeout, 257  
    hostport, 258  
    key, 258  
    parse\_type, 258  
    queue, 259  
    retry\_read, 259  
    retry\_write, 259  
    send\_request, 257  
    set\_state, 257  
        start, 257  
        state, 259  
        ta, 259  
        timeout, 259  
        tls, 259  
        tls\_connect, 257  
rpki::https::http\_listener, 260  
    \_\_init\_\_, 261  
    cert, 262  
    dynamic\_ta, 262  
    handle\_accept, 261  
    handle\_error, 261  
    handlers, 262  
    key, 262  
    log, 262  
    ta, 262  
rpki::https::http\_message, 263  
    \_\_init\_\_, 264  
    \_\_str\_\_, 264  
    body, 266  
    format, 264  
    headers, 266  
    normalize\_headers, 265  
    parse\_from\_wire, 265  
    parse\_version, 265  
    persistent, 265  
    software\_name, 266  
    version, 266  
rpki::https::http\_queue, 266  
    \_\_init\_\_, 268  
    cert, 269  
    client, 269  
    detach, 268  
    hostport, 270  
    key, 270  
    log, 270  
    queue, 270  
    request, 268  
    restart, 269  
    return\_result, 269  
    send\_request, 269  
    ta, 270  
rpki::https::http\_request, 270  
    \_\_init\_\_, 272  
    callback, 273  
    cmd, 273

errback, 273  
format\_first\_line, 272  
parse\_first\_line, 272  
path, 273  
retried, 273  
rpki::https::http\_response, 273  
    \_\_init\_\_, 275  
    code, 275  
    format\_first\_line, 275  
    parse\_first\_line, 275  
    reason, 275  
rpki::https::http\_server, 276  
    \_\_init\_\_, 278  
    expect\_close, 280  
    find\_handler, 278  
    handle\_message, 278  
    handle\_no\_content\_length, 279  
    handlers, 280  
    parse\_type, 280  
    retry\_read, 280  
    retry\_write, 280  
    send\_error, 279  
    send\_message, 279  
    send\_reply, 279  
    timeout, 281  
    tls, 281  
    tls\_accept, 279  
rpki::https::http\_stream, 281  
    \_\_init\_\_, 284  
    buffer, 289  
    chunk\_body, 284  
    chunk\_discard\_crlf, 284  
    chunk\_discard\_trailer, 284  
    chunk\_handler, 289  
    chunk\_header, 284  
    close, 284  
    collect\_incoming\_data, 285  
    found\_terminator, 285  
    get\_buffer, 285  
    handle\_body, 285  
    handle\_close, 286  
    handle\_error, 286  
    handle\_read, 286  
    handle\_timeout, 286  
    handle\_write, 287  
    initiate\_send, 287  
log, 289  
log\_cert, 287  
msg, 289  
readable, 287  
recv, 287  
restart, 288  
retry\_read, 289  
retry\_write, 289  
send, 288  
timer, 289  
tls, 290  
update\_timeout, 288  
writeable, 288  
rpki::ipaddrs::v4addr, 290  
    \_\_new\_\_, 291  
    \_\_str\_\_, 291  
    bits, 292  
    from\_bytes, 291  
    to\_bytes, 291  
rpki::ipaddrs::v6addr, 292  
    \_\_new\_\_, 294  
    \_\_str\_\_, 294  
    bits, 294  
    from\_bytes, 294  
    to\_bytes, 294  
rpki::left\_right  
    enforce\_strict\_up\_down\_xml\_-  
        sender, 82  
rpki::left\_right::bsc\_elt, 295  
    attributes, 298  
    booleans, 298  
    children, 297  
    element\_name, 299  
    elements, 299  
    handles, 299  
    parents, 297  
    pkcs10\_request, 299  
    private\_key\_id, 299  
    repositories, 298  
    serve\_pre\_save\_hook, 298  
    signing\_cert, 299  
    signing\_cert\_crl, 300  
    sql\_template, 300  
rpki::left\_right::child\_elt, 300  
    attributes, 304  
    booleans, 304

bpkı\_cert, 304  
bpkı\_glue, 304  
ca\_from\_class\_name, 302  
child\_certs, 302  
clear\_https\_ta\_cache, 304  
element\_name, 304  
elements, 305  
endElement, 303  
handles, 305  
parents, 303  
serve\_destroy\_hook, 303  
serve\_post\_save\_hook, 303  
serve\_up\_down, 303  
sql\_template, 305  
rpki::left\_right::cms\_msg, 305  
encoding, 307  
saxify, 307  
schema, 307  
rpki::left\_right::data\_elt, 307  
bsc, 309  
handles, 311  
make\_reply\_clone\_hook, 309  
self, 309  
self\_handle, 311  
self\_id, 311  
serve\_fetch\_all, 310  
serve\_fetch\_handle, 310  
serve\_fetch\_one\_maybe, 310  
serve\_pre\_save\_hook, 310  
rpki::left\_right::left\_right\_namespace, 311  
nsmap, 312  
xmlns, 312  
rpki::left\_right::list\_published\_objects\_elt, 313  
attributes, 316  
element\_name, 316  
make\_reply, 315  
obj, 316  
serve\_dispatch, 315  
text\_attribute, 316  
rpki::left\_right::list\_received\_resources\_elt, 316  
attributes, 318  
element\_name, 318  
make\_reply, 318  
serve\_dispatch, 318  
attributes, 322  
element\_name, 322  
ip4, 322  
ip6, 322  
startElement, 321  
toXML, 321  
valid\_until, 322  
rpki::left\_right::list\_roa\_requests\_elt, 323  
attributes, 324  
element\_name, 324  
ip4, 325  
ip6, 325  
startElement, 324  
rpki::left\_right::msg, 325  
pdus, 327  
serve\_top\_level, 327  
version, 327  
rpki::left\_right::parent\_elt, 328  
attributes, 332  
booleans, 332  
bpki\_cms\_cert, 332  
bpki\_cms\_glue, 332  
bpki\_https\_cert, 333  
bpki\_https\_glue, 333  
cas, 330  
element\_name, 333  
elements, 333  
handles, 333  
query\_up\_down, 330  
repository, 331  
serve\_post\_save\_hook, 331  
serve\_rekey, 331  
serve\_revoke, 331  
serve\_revoke\_forgotten, 331  
sql\_template, 333  
rpki::left\_right::report\_error\_elt, 334  
attributes, 337  
element\_name, 337  
error\_code, 337  
error\_text, 337  
from\_exception, 336  
self\_handle, 337  
tag, 337

text\_attribute, 337  
rpki::left\_right::repository\_elt, 338  
    attributes, 341  
    bpki\_cert, 341  
    bpki\_glue, 341  
    call\_pubd, 340  
    default\_pubd\_handler, 340  
    element\_name, 341  
    elements, 342  
    handles, 342  
    parents, 341  
    sql\_template, 342  
rpki::left\_right::sax\_handler, 342  
    name, 344  
    pdu, 344  
    version, 344  
rpki::left\_right::self\_elt, 344  
    attributes, 351  
    booleans, 351  
    bpki\_cert, 351  
    bpki\_glue, 351  
    bscs, 347  
    children, 347  
    client\_poll, 347  
    crl\_interval, 352  
    cron, 347  
    element\_name, 352  
    elements, 352  
    handles, 352  
    parents, 347  
    regen\_margin, 352  
    regenerate\_crls\_and\_manifests, 348  
    repositories, 348  
    roas, 348  
    serve\_fetch\_all, 348  
    serve\_fetch\_handle, 349  
    serve\_fetch\_one\_maybe, 349  
    serve\_post\_save\_hook, 349  
    serve\_publish\_world\_now, 349  
    serve\_rekey, 350  
    serve\_revocate, 350  
    serve\_revocate\_forgotten, 350  
    serve\_run\_now, 350  
    sql\_template, 352  
    update\_children, 350  
    update\_roas, 351  
use\_hsm, 353  
rpki::log  
    debug, 84  
    enable\_trace, 84  
    error, 84  
    info, 84  
    init, 83  
    note, 85  
    pid, 85  
    set\_trace, 83  
    tag, 85  
    trace, 84  
    traceback, 84  
    use\_syslog, 85  
    warn, 85  
rpki::log::logger, 353  
    \_\_call\_\_, 354  
    \_\_init\_\_, 354  
    priority, 354  
rpki::manifest::FileAndHash, 355  
    \_\_init\_\_, 356  
    file, 356  
    hash, 356  
rpki::manifest::FilesAndHashes, 356  
    \_\_init\_\_, 357  
rpki::manifest::Manifest, 358  
    \_\_init\_\_, 359  
    explicitVersion, 359  
    fileHashAlg, 359  
    fileList, 359  
    manifestNumber, 359  
    nextUpdate, 359  
    thisUpdate, 360  
    version, 360  
rpki::oids  
    name2oid, 87  
    oid2name, 87  
rpki::publication::certificate\_elt, 360  
    element\_name, 362  
    payload\_type, 362  
rpki::publication::client\_elt, 362  
    attributes, 365  
    base\_uri, 365  
    bpki\_cert, 366  
    bpki\_glue, 366  
    check\_allowed\_uri, 364

clear\_https\_ta\_cache, 366  
element\_name, 366  
elements, 366  
endElement, 364  
serve\_fetch\_all, 365  
serve\_fetch\_one\_maybe, 365  
serve\_post\_save\_hook, 365  
sql\_template, 366  
rpki::publication::cms\_msg, 367  
    encoding, 369  
    saxify, 369  
    schema, 369  
rpki::publication::config\_elt, 369  
    attributes, 372  
    config\_id, 372  
    element\_name, 373  
    elements, 373  
    fetch, 371  
    serve\_fetch\_one\_maybe, 371  
    serve\_set, 372  
    sql\_template, 373  
    startElement, 372  
    wired\_in\_config\_id, 373  
rpki::publication::control\_elt, 373  
    serve\_dispatch, 376  
rpki::publication::crl\_elt, 376  
    element\_name, 378  
    payload\_type, 378  
rpki::publication::manifest\_elt, 378  
    element\_name, 380  
    payload\_type, 380  
rpki::publication::msg, 380  
    pdus, 382  
    serve\_top\_level, 382  
    version, 382  
rpki::publication::publication\_-  
    namespace, 383  
    nsmap, 384  
    xmlns, 384  
rpki::publication::publication\_object\_elt,  
    384  
    attributes, 388  
    endElement, 386  
    make\_publish, 386  
    make\_withdraw, 387  
    payload, 388  
payload\_type, 388  
raise\_if\_error, 387  
serve\_dispatch, 387  
serve\_publish, 387  
serve\_withdraw, 387  
toXML, 388  
uri\_to\_filename, 388  
rpki::publication::report\_error\_elt, 389  
    \_\_str\_\_, 391  
    attributes, 392  
    element\_name, 392  
    error\_code, 392  
    error\_text, 392  
    from\_exception, 391  
    raise\_if\_error, 392  
    tag, 393  
    text\_attribute, 393  
rpki::publication::roa\_elt, 393  
    element\_name, 395  
    payload\_type, 395  
rpki::publication::sax\_handler, 395  
    name, 397  
    pdu, 397  
    version, 397  
rpki::relaxng  
    left\_right, 89  
    publication, 89  
    up\_down, 89  
rpki::resource\_set  
    \_\_bs2long, 91  
    \_\_long2bs, 91  
    \_\_rsplit, 91  
    inherit\_token, 92  
    test1, 92  
    test2, 92  
rpki::resource\_set::resource\_bag, 397  
    \_\_eq\_\_, 399  
    \_\_init\_\_, 399  
    \_\_ne\_\_, 399  
    \_\_str\_\_, 400  
    asn, 401  
    empty, 400  
    from\_rfc3779\_tuples, 400  
    intersection, 400  
    oversized, 400  
    undersized, 400

union, 401  
v4, 401  
v6, 401  
valid\_until, 401  
rpki::resource\_set::resource\_range, 402  
    \_\_cmp\_\_, 403  
    \_\_init\_\_, 403  
    max, 403  
    min, 403  
rpki::resource\_set::resource\_range\_as, 404  
    \_\_str\_\_, 405  
    datum\_type, 405  
    min, 406  
    to\_rfc3779\_tuple, 405  
rpki::resource\_set::resource\_range\_ip, 406  
    \_\_str\_\_, 408  
    \_prefixlen, 408  
    make\_prefix, 408  
    to\_rfc3779\_tuple, 408  
rpki::resource\_set::resource\_range\_ipv4, 409  
    datum\_type, 411  
rpki::resource\_set::resource\_range\_ipv6, 411  
    datum\_type, 413  
rpki::resource\_set::resource\_set, 413  
    \_\_init\_\_, 415  
    \_\_str\_\_, 415  
    \_comm, 415  
    contains, 416  
    difference, 416  
    from\_sql, 416  
    inherit, 417  
    intersection, 416  
    issubset, 416  
    issuperset, 417  
    symmetric\_difference, 417  
    union, 417  
rpki::resource\_set::resource\_set\_as, 418  
    inherit, 420  
    parse\_rfc3779\_tuple, 419  
    parse\_str, 419  
    range\_type, 420  
    to\_rfc3779\_tuple, 419  
rpki::resource\_set::resource\_set\_ip, 420  
    inherit, 423  
    parse\_rfc3779\_tuple, 422  
    parse\_str, 422  
    to\_rfc3779\_tuple, 422  
rpki::resource\_set::resource\_set\_ipv4, 423  
    afi, 425  
    range\_type, 425  
rpki::resource\_set::resource\_set\_ipv6, 425  
    afi, 427  
    range\_type, 427  
rpki::resource\_set::roa\_prefix, 427  
    \_\_cmp\_\_, 429  
    \_\_init\_\_, 429  
    \_\_str\_\_, 429  
    max, 429  
    max\_prefixlen, 430  
    min, 430  
    prefix, 430  
    prefixlen, 431  
    to\_resource\_range, 430  
    to\_roa\_tuple, 430  
rpki::resource\_set::roa\_prefix\_ipv4, 431  
    range\_type, 433  
rpki::resource\_set::roa\_prefix\_ipv6, 433  
    range\_type, 435  
rpki::resource\_set::roa\_prefix\_set, 435  
    \_\_init\_\_, 437  
    \_\_str\_\_, 437  
    from\_sql, 437  
    parse\_str, 437  
    to\_resource\_set, 437  
    to\_roa\_tuple, 438  
rpki::resource\_set::roa\_prefix\_set\_ipv4, 438  
    prefix\_type, 440  
    resource\_set\_type, 440  
rpki::resource\_set::roa\_prefix\_set\_ipv6, 440  
    prefix\_type, 442  
    resource\_set\_type, 442  
rpki::roa::ROAIPAddress, 442  
    \_\_init\_\_, 443  
    address, 444

maxLength, 444  
rpki::roa::ROAIPAddresses, 444  
    \_\_init\_\_, 445  
rpki::roa::ROAIPAddressFamilies, 445  
    \_\_init\_\_, 446  
rpki::roa::ROAIPAddressFamily, 446  
    \_\_init\_\_, 447  
        addresses, 448  
        addressFamily, 448  
rpki::roa::RouteOriginAttestation, 448  
    \_\_init\_\_, 449  
        asID, 449  
        explicitVersion, 449  
        ipAddrBlocks, 449  
        version, 449  
rpki::rpki\_engine::ca\_detail\_obj, 450  
    activate, 453  
    ca, 453  
    ca\_cert\_uri, 457  
    ca\_id, 457  
    child\_certs, 453  
    create, 453  
    crl\_published, 457  
    crl\_published\_callback, 453  
    crl\_uri, 453  
    crl\_uri\_tail, 454  
    delete, 454  
    gctx, 457  
    generate\_crl, 454  
    generate\_manifest, 454  
    generate\_manifest\_cert, 454  
    issue, 455  
    issue\_ee, 455  
    latest\_ca\_cert, 457  
    latest\_crl, 457  
    latest\_manifest, 458  
    latest\_manifest\_cert, 458  
    manifest\_private\_key\_id, 458  
    manifest\_public\_key, 458  
    manifest\_published, 458  
    manifest\_published\_callback, 455  
    manifest\_uri, 455  
    nextUpdate, 458  
    private\_key\_id, 458  
    public\_key, 459  
    revoke, 455  
        revoked\_certs, 456  
        roas, 456  
        sql\_decode, 456  
        sql\_template, 459  
        state, 459  
        update, 456  
rpki::rpki\_engine::ca\_obj, 459  
    ca\_details, 461  
    check\_for\_updates, 461  
    construct\_sia\_uri, 462  
    create, 462  
    delete, 462  
    fetch\_active, 462  
    fetch\_DEPRECATED, 463  
    fetch\_issue\_response\_candidates, 463  
    fetch\_pending, 463  
    fetch\_revoked, 463  
    gctx, 465  
    last\_crl\_sn, 465  
    last\_issued\_sn, 465  
    last\_manifest\_sn, 465  
    next\_crl\_number, 463  
    next\_manifest\_number, 464  
    next\_serial\_number, 464  
    parent, 464  
    parent\_id, 465  
    parent\_resource\_class, 465  
    rekey, 464  
    revoke, 464  
    sia\_uri, 466  
    sql\_template, 466  
rpki::rpki\_engine::child\_cert\_obj, 466  
    \_\_init\_\_, 468  
    ca\_detail, 468  
    ca\_detail\_id, 470  
    cert, 470  
    child, 468  
    child\_id, 470  
    fetch, 469  
    gctx, 470  
    published, 470  
    published\_callback, 469  
    reissue, 469  
    revoke, 469  
    sql\_template, 471

uri, 469  
uri\_tail, 470  
rpki::rpki\_engine::publication\_queue,  
    471  
    \_\_init\_\_, 473  
    \_\_add, 473  
    call\_pubd, 473  
    handlers, 474  
    msgs, 474  
    publish, 473  
    replace, 474  
    repositories, 474  
    uris, 474  
    withdraw, 474  
rpki::rpki\_engine::revoked\_cert\_obj, 475  
    \_\_init\_\_, 476  
    ca\_detail, 476  
    ca\_detail\_id, 477  
    expires, 477  
    gctx, 477  
    revoke, 476  
    revoked, 477  
    serial, 477  
    sql\_template, 477  
rpki::rpki\_engine::roa\_obj, 478  
    \_\_init\_\_, 480  
    asn, 483  
    ca\_detail, 480  
    ca\_detail\_id, 483  
    cert, 483  
    gctx, 484  
    generate, 481  
    ipv4, 484  
    ipv6, 484  
    published, 484  
    published\_callback, 481  
    regenerate, 481  
    revoke, 481  
    roa, 484  
    self, 482  
    self\_id, 484  
    sql\_delete\_hook, 482  
    sql\_fetch\_hook, 482  
    sql\_insert\_hook, 482  
    sql\_template, 484  
    update, 483  
                uri, 483  
                uri\_tail, 483  
                rpki::rpki\_engine::rpkid\_context, 485  
                \_\_init\_\_, 488  
                bpki\_ta, 490  
                build\_https\_ta\_cache, 488  
                checkpoint, 488  
                clear\_https\_ta\_cache, 488  
                cron, 488  
                cron\_keepalive, 490  
                cron\_period, 490  
                cron\_timeout, 490  
                cron\_timer, 490  
                cronjob\_handler, 488  
                https\_server\_host, 491  
                https\_server\_port, 491  
                https\_ta\_cache, 491  
                initial\_delay, 491  
                irbe\_cert, 491  
                irdb\_cert, 491  
                irdb\_query, 489  
                irdb\_query\_child\_resources, 489  
                irdb\_query\_roa\_requests, 489  
                irdb\_url, 491  
                left\_right\_handler, 489  
                publication\_kludge\_base, 492  
                rpkid\_cert, 492  
                rpkid\_key, 492  
                sql, 492  
                start\_cron, 489  
                up\_down\_handler, 490  
                up\_down\_url\_regex, 492  
                use\_internal\_cron, 492  
rpki::sql::session, 493  
    \_\_init\_\_, 495  
    \_exceptions\_enabled, 496  
    \_wrap\_execute, 495  
    assert\_pristine, 495  
    cache, 497  
    cache\_clear, 495  
    close, 495  
    connect, 495  
    cur, 497  
    database, 497  
    db, 497  
    dirty, 497

execute, 495  
executemany, 496  
fetchall, 496  
lastrowid, 496  
password, 497  
ping, 496  
sweep, 496  
username, 497  
rpki::sql::sql\_persistent, 498  
    gctx, 504  
    sql\_debug, 504  
    sql\_decode, 500  
    sql\_delete, 501  
    sql\_delete\_hook, 501  
    sql\_deleted, 504  
    sql\_encode, 501  
    sql\_fetch, 501  
    sql\_fetch\_all, 502  
    sql\_fetch\_hook, 502  
    sql\_fetch\_where, 502  
    sql\_fetch\_where1, 502  
    sql\_in\_db, 505  
    sql\_init, 502  
    sql\_insert\_hook, 503  
    sql\_is\_dirty, 503  
    sql\_mark\_clean, 503  
    sql\_mark\_deleted, 503  
    sql\_mark\_dirty, 503  
    sql\_store, 504  
    sql\_update\_hook, 504  
rpki::sql::template, 505  
    \_\_init\_\_, 507  
    columns, 507  
    delete, 507  
    index, 507  
    insert, 507  
    map, 508  
    select, 508  
    table, 508  
    update, 508  
rpki::sundial  
    \_cast, 96  
    now, 96  
    test, 96  
rpki::sundial::datetime, 508  
    \_\_add\_\_, 510  
        \_\_radd\_\_, 510  
        \_\_rsub\_\_, 510  
        \_\_str\_\_, 511  
        \_\_sub\_\_, 511  
        earlier, 511  
        from\_sql, 511  
        fromASN1tuple, 511  
        fromdatetime, 511  
        fromGeneralizedTime, 512  
        fromUTCTime, 512  
        fromXMLtime, 512  
        later, 512  
        PKIX\_threshhold, 514  
        to\_sql, 512  
        toASN1tuple, 513  
        toGeneralizedTime, 513  
        totimestamp, 513  
        toUTCTime, 513  
        toXMLtime, 513  
rpki::sundial::timedelta, 514  
    \_\_abs\_\_, 517  
    \_\_add\_\_, 517  
    \_\_div\_\_, 517  
    \_\_floordiv\_\_, 517  
    \_\_mul\_\_, 517  
    \_\_neg\_\_, 517  
    \_\_pos\_\_, 517  
    \_\_radd\_\_, 517  
    \_\_rdiv\_\_, 518  
    \_\_rfloordiv\_\_, 518  
    \_\_rmul\_\_, 518  
    \_\_rsub\_\_, 518  
    \_\_sub\_\_, 518  
    convert\_to\_seconds, 518  
    fromtimedelta, 518  
    parse, 519  
    regexp, 519  
    years\_to\_seconds, 519  
rpki::up\_down  
    nsmap, 98  
    xmlns, 98  
rpki::up\_down::base\_elt, 520  
    check\_response, 521  
    endElement, 521  
    make\_b64elt, 521  
    make\_elt, 521

serve\_pdu, 522  
startElement, 522  
rpki::up\_down::certificate\_elt, 522  
cert, 525  
cert\_url, 525  
endElement, 524  
req\_resource\_set\_as, 525  
req\_resource\_set\_ipv4, 525  
req\_resource\_set\_ipv6, 525  
startElement, 524  
toXML, 524  
rpki::up\_down::class\_elt, 525  
\_\_init\_\_, 527  
cert\_url, 528  
certs, 528  
class\_name, 528  
endElement, 527  
from\_resource\_bag, 527  
issuer, 529  
resource\_set\_as, 529  
resource\_set\_ipv4, 529  
resource\_set\_ipv6, 529  
resource\_set\_notafter, 529  
startElement, 528  
suggested\_sia\_head, 529  
to\_resource\_bag, 528  
toXML, 528  
rpki::up\_down::class\_response\_syntax,  
    530  
    \_\_init\_\_, 531  
    classes, 532  
    startElement, 531  
    toXML, 531  
rpki::up\_down::cms\_msg, 532  
    encoding, 534  
    saxify, 534  
    schema, 534  
rpki::up\_down::error\_response\_pdu, 534  
    \_\_init\_\_, 536  
    check\_response, 536  
    codes, 537  
    description, 537  
    endElement, 536  
    exceptions, 537  
    status, 537  
    toXML, 537  
rpki::up\_down::issue\_pdu, 538  
    class\_name, 541  
    endElement, 540  
    pkcs10, 541  
    query, 540  
    req\_resource\_set\_as, 541  
    req\_resource\_set\_ipv4, 541  
    req\_resource\_set\_ipv6, 541  
    serve\_pdu, 540  
    startElement, 540  
    toXML, 541  
rpki::up\_down::issue\_response\_pdu, 542  
    check\_response, 544  
rpki::up\_down::list\_pdu, 544  
    query, 546  
    serve\_pdu, 546  
    toXML, 546  
rpki::up\_down::list\_response\_pdu, 547  
rpki::up\_down::message\_pdu, 548  
    \_\_str\_\_, 550  
    log\_query, 550  
    make\_query, 550  
    name2type, 552  
    payload, 552  
    recipient, 552  
    sender, 552  
    serve\_error, 551  
    serve\_top\_level, 551  
    startElement, 551  
    toXML, 551  
    type, 552  
    type2name, 552  
    version, 553  
rpki::up\_down::multi\_uri, 553  
    \_\_init\_\_, 554  
    \_\_str\_\_, 555  
    rsync, 555  
rpki::up\_down::revoke\_pdu, 555  
    class\_name, 558  
    get\_SKI, 557  
    query, 557  
    serve\_pdu, 557  
    ski, 558  
rpki::up\_down::revoke\_response\_pdu,  
    558  
rpki::up\_down::revoke\_syntax, 560

class\_name, 561  
    ski, 561  
    startElement, 561  
    toXML, 561  
rpk:::up\_down::sax\_handler, 562  
    name, 564  
    pdu, 564  
    version, 564  
rpki:::x509  
    \_find\_xia\_uri, 100  
    calculate\_SKI, 100  
    POWify\_OID, 100  
rpki:::x509::CMS\_object, 564  
    content, 568  
    debug\_cms\_certs, 568  
    DER, 569  
    dump\_on\_verify\_failure, 569  
    econtent\_oid, 569  
    extract, 567  
    formats, 569  
    get\_content, 567  
    get\_DER, 567  
    get\_POW, 567  
    other\_clear, 569  
    pem\_converter, 570  
    POW, 570  
    print\_on\_der\_error, 570  
    require\_crls, 570  
    set\_content, 568  
    sign, 568  
    verify, 568  
rpki:::x509::CRL, 571  
    DER, 574  
    formats, 574  
    generate, 572  
    get\_DER, 572  
    get\_POW, 573  
    get\_POWpkix, 573  
    getIssuer, 573  
    getNextUpdate, 573  
    getThisUpdate, 573  
    pem\_converter, 574  
    POW, 574  
    POWpkix, 574  
rpki:::x509::DeadDrop, 575  
    \_\_init\_\_, 576  
                dump, 576  
                maildir, 576  
                pid, 576  
                rpki:::x509::DER\_CMS\_object, 577  
                        content, 578  
                        decode, 578  
                        encode, 578  
                rpki:::x509::DER\_object, 579  
                        \_\_cmp\_\_, 581  
                        \_\_init\_\_, 581  
                        clear, 581  
                        DER, 586  
                        dumpasn1, 581  
                        empty, 581  
                        formats, 586  
                        from\_sql, 582  
                        gAKI, 582  
                        get\_3779resources, 582  
                        get\_AIA, 582  
                        get\_aia\_uri, 582  
                        get\_AKI, 583  
                        get\_Base64, 583  
                        get\_basicConstraints, 583  
                        get\_DER, 583  
                        get\_PEM, 583  
                        get\_SIA, 584  
                        get\_sia\_directory\_uri, 584  
                        get\_sia\_manifest\_uri, 584  
                        get\_SKI, 584  
                        gSKI, 584  
                        hAKI, 585  
                        hSKI, 585  
                        is\_CA, 585  
                        other\_clear, 586  
                        pem\_converter, 586  
                        set, 585  
                        to\_sql, 585  
rpki:::x509::PEM\_converter, 587  
    \_\_init\_\_, 588  
    b, 589  
    e, 589  
    looks\_like\_PEM, 588  
    to\_DER, 588  
    to\_PEM, 588  
rpki:::x509::PKCS10, 589  
    check\_valid\_rpki, 591

create, 591  
create\_ca, 591  
DER, 592  
formats, 592  
get\_DER, 592  
get\_POWpkix, 592  
getPublicKey, 592  
pem\_converter, 593  
POWpkix, 593  
rpki::x509::ROA, 593  
    build, 595  
    content\_class, 595  
    econtent\_oid, 595  
    pem\_converter, 595  
rpki::x509::RSA, 596  
    DER, 599  
    formats, 599  
    generate, 598  
    get\_DER, 598  
    get\_POW, 598  
    get\_public\_DER, 599  
    get\_RSAPublic, 599  
    get\_SKI, 599  
    pem\_converter, 600  
    POW, 600  
rpki::x509::RSAPublic, 600  
    DER, 603  
    formats, 603  
    get\_DER, 602  
    get\_POW, 602  
    get\_SKI, 602  
    pem\_converter, 603  
    POW, 603  
rpki::x509::SignedManifest, 604  
    build, 605  
    content\_class, 606  
    econtent\_oid, 606  
    getNextUpdate, 605  
    getThisUpdate, 605  
    pem\_converter, 606  
rpki::x509::X509, 606  
    cross\_certify, 608  
    DER, 611  
    expired, 609  
    formats, 611  
    get\_DER, 609  
get\_POW, 609  
get\_POWpkix, 609  
getIssuer, 609  
getNotAfter, 609  
getNotBefore, 610  
getPublicKey, 610  
getSerial, 610  
getSubject, 610  
issue, 610  
normalize\_chain, 611  
pem\_converter, 611  
POW, 612  
POWpkix, 612  
rpki::x509::XML\_CMS\_object, 612  
    content, 616  
    decode, 614  
    dump\_inbound\_cms, 616  
    dump\_outbound\_cms, 616  
    dump\_to\_disk, 614  
    econtent\_oid, 616  
    encode, 614  
    pretty\_print\_content, 615  
    schema\_check, 615  
    unwrap, 615  
    wrap, 615  
rpki::xml\_utils::base\_elt, 616  
    \_\_str\_\_, 618  
    attributes, 620  
    booleans, 620  
    elements, 620  
    endElement, 618  
    make\_b64elt, 619  
    make\_elt, 619  
    make\_pdu, 619  
    readAttrs, 619  
    startElement, 619  
    toXML, 620  
rpki::xml\_utils::data\_elt, 621  
    endElement, 623  
    make\_reply, 623  
    make\_reply\_clone\_hook, 623  
    serve\_create, 624  
    serve\_destroy, 624  
    serve\_destroy\_hook, 624  
    serve\_dispatch, 624  
    serve\_fetch\_one, 624

serve\_get, 625  
serve\_list, 625  
serve\_post\_save\_hook, 625  
serve\_pre\_save\_hook, 625  
serve\_set, 625  
toXML, 626  
unimplemented\_control, 626  
rpki::xml\_utils::msg, 626  
    \_\_str\_\_, 628  
    endElement, 628  
    is\_query, 628  
    is\_reply, 628  
    query, 628  
    reply, 629  
    startElement, 629  
    toXML, 629  
    type, 629  
    version, 629  
rpki::xml\_utils::sax\_handler, 630  
    \_\_init\_\_, 631  
    characters, 631  
    create\_top\_level, 632  
    endElement, 632  
    endElementNS, 632  
    result, 633  
    saxify, 632  
    stack, 633  
    startElement, 632  
    startElementNS, 633  
    text, 633  
rpki::xml\_utils::text\_elt, 634  
    endElement, 635  
    text\_attribute, 635  
    toXML, 635  
rpki\_base\_uri  
    rootd, 65  
rpki\_class\_name  
    rootd, 66  
rpki\_content\_type  
    rpki::https, 79  
rpki\_engine.py(3107), 651  
rpki\_root\_cert  
    rootd, 66  
rpki\_root\_cert\_file  
    rootd, 66  
rpki\_root\_cert\_uri  
    rootd, 66  
rpki\_root\_crl  
    rootd, 66  
rpki\_root\_dir  
    rootd, 66  
rpki\_root\_key  
    rootd, 66  
rpki\_root\_manifest  
    rootd, 67  
rpki\_subject\_cert  
    rootd, 67  
rpki\_subject\_lifetime  
    rootd, 67  
rpki\_subject\_pkcs10  
    rootd, 67  
rpki\_subject\_regen  
    rootd, 67  
rpkid, 101  
    cfg\_file, 102  
    main, 102  
    profile, 102  
rpkid.py(2913), 651  
rpkid\_cert  
    irdbd, 58  
    rpki::rpki\_engine::rpkid\_context,  
        492  
rpkid\_key  
    rpki::rpki\_engine::rpkid\_context,  
        492  
rsync  
    rpki::up\_down::multi\_uri, 555  
run\_debug  
    rpki::async::timer, 184  
run\_deferred  
    rpki::async, 70  
runq  
    rpki::async::timer, 182  
saxify  
    irbe\_cli::left\_right\_cms\_msg, 123  
    irbe\_cli::publication\_cms\_msg, 138  
    rootd::cms\_msg, 160  
    rpki::left\_right::cms\_msg, 307  
    rpki::publication::cms\_msg, 369  
    rpki::up\_down::cms\_msg, 534  
    rpki::xml\_utils::sax\_handler, 632

schema  
    rpki::left\_right::cms\_msg, 307  
    rpki::publication::cms\_msg, 369  
    rpki::up\_down::cms\_msg, 534  
schema\_check  
    rpki::x509::XML\_CMS\_object, 615  
seconds\_until\_wakeup  
    rpki::async::timer, 182  
select  
    rpki::sql::template, 508  
self  
    rpki::left\_right::data\_elt, 309  
    rpki::rpk\_engine::roa\_obj, 482  
self\_handle  
    rpki::left\_right::data\_elt, 311  
    rpki::left\_right::report\_error\_elt, 337  
self\_id  
    rpki::left\_right::data\_elt, 311  
    rpki::rpk\_engine::roa\_obj, 484  
send  
    rpki::https::http\_stream, 288  
send\_error  
    rpki::https::http\_server, 279  
send\_message  
    rpki::https::http\_server, 279  
send\_reply  
    rpki::https::http\_server, 279  
send\_request  
    rpki::https::http\_client, 257  
    rpki::https::http\_queue, 269  
sender  
    rpki::up\_down::message\_pdu, 552  
Sequence, 636  
SequenceOf, 636  
serial  
    rpki::rpk\_engine::revoked\_cert\_obj, 477  
serve\_create  
    rpki::xml\_utils::data\_elt, 624  
serve\_destroy  
    rpki::xml\_utils::data\_elt, 624  
serve\_destroy\_hook  
    rpki::left\_right::child\_elt, 303  
    rpki::xml\_utils::data\_elt, 624  
serve\_dispatch  
    rpki::left\_right::list\_published\_objects\_elt, 315  
    rpki::left\_right::list\_received\_resources\_elt, 318  
    rpki::publication::control\_elt, 376  
    rpki::publication::publication\_object\_elt, 387  
    rpki::xml\_utils::data\_elt, 624  
serve\_error  
    rpki::up\_down::message\_pdu, 551  
serve\_fetch\_all  
    rpki::left\_right::data\_elt, 310  
    rpki::left\_right::self\_elt, 348  
    rpki::publication::client\_elt, 365  
serve\_fetch\_handle  
    rpki::left\_right::data\_elt, 310  
    rpki::left\_right::self\_elt, 349  
serve\_fetch\_one  
    rpki::xml\_utils::data\_elt, 624  
serve\_fetch\_one\_maybe  
    rpki::left\_right::data\_elt, 310  
    rpki::left\_right::self\_elt, 349  
    rpki::publication::client\_elt, 365  
    rpki::publication::config\_elt, 371  
serve\_get  
    rpki::xml\_utils::data\_elt, 625  
serve\_list  
    rpki::xml\_utils::data\_elt, 625  
serve\_pdu  
    rootd::issue\_pdu, 162  
    rootd::list\_pdu, 164  
    rootd::revoke\_pdu, 168  
    rpki::up\_down::base\_elt, 522  
    rpki::up\_down::issue\_pdu, 540  
    rpki::up\_down::list\_pdu, 546  
    rpki::up\_down::revoke\_pdu, 557  
serve\_post\_save\_hook  
    rpki::left\_right::child\_elt, 303  
    rpki::left\_right::parent\_elt, 331  
    rpki::left\_right::self\_elt, 349  
    rpki::publication::client\_elt, 365  
    rpki::xml\_utils::data\_elt, 625  
serve\_pre\_save\_hook  
    rpki::left\_right::bsc\_elt, 298  
    rpki::left\_right::data\_elt, 310  
    rpki::xml\_utils::data\_elt, 625

serve\_publish  
    rpki::publication::publication\_object\_elt, 387  
serve\_publish\_world\_now  
    rpki::left\_right::self\_elt, 349  
serve\_rekey  
    rpki::left\_right::parent\_elt, 331  
    rpki::left\_right::self\_elt, 350  
serve\_revoke  
    rpki::left\_right::parent\_elt, 331  
    rpki::left\_right::self\_elt, 350  
serve\_revoke\_forgotten  
    rpki::left\_right::parent\_elt, 331  
    rpki::left\_right::self\_elt, 350  
serve\_run\_now  
    rpki::left\_right::self\_elt, 350  
serve\_set  
    rpki::publication::config\_elt, 372  
    rpki::xml\_utils::data\_elt, 625  
serve\_top\_level  
    rpki::left\_right::msg, 327  
    rpki::publication::msg, 382  
    rpki::up\_down::message\_pdu, 551  
serve\_up\_down  
    rpki::left\_right::child\_elt, 303  
serve\_withdraw  
    rpki::publication::publication\_object\_elt, 387  
server  
    rpki::https, 77  
server\_cert  
    irdbd, 58  
    rootd, 67  
    rpki::https::caller, 253  
server\_ta  
    rpki::https::caller, 253  
set  
    rpki::async::timer, 182  
    rpki::x509::DER\_object, 585  
set\_content  
    rpki::x509::CMS\_object, 568  
set\_errback  
    rpki::async::timer, 183  
set\_global\_flags  
    rpki::config::parser, 193  
set\_handler  
    rpki::async::timer, 183  
set\_state  
    rpki::https::http\_client, 257  
set\_subject\_cert  
    rootd, 63  
set\_subject\_pkcs10  
    rootd, 63  
set\_trace  
    rpki::log, 83  
sia\_uri  
    rpki::rpki\_engine::ca\_obj, 466  
sign  
    rpki::x509::CMS\_object, 568  
signing\_cert  
    irbe\_cli::bsc\_elt, 106  
    rpki::left\_right::bsc\_elt, 299  
signing\_cert\_crl  
    irbe\_cli::bsc\_elt, 106  
    rpki::left\_right::bsc\_elt, 300  
ski  
    rpki::up\_down::revoke\_pdu, 558  
    rpki::up\_down::revoke\_syntax, 561  
software\_name  
    rpki::https::http\_message, 266  
sql  
    pubd::pubd\_context, 158  
    rpki::rpki\_engine::rpkid\_context, 492  
sql.py(2895), 652  
sql\_debug  
    rpki::sql::sql\_persistent, 504  
sql\_decode  
    rpki::rpki\_engine::ca\_detail\_obj, 456  
    rpki::sql::sql\_persistent, 500  
sql\_delete  
    rpki::sql::sql\_persistent, 501  
sql\_delete\_hook  
    rpki::rpki\_engine::roa\_obj, 482  
    rpki::sql::sql\_persistent, 501  
sql\_deleted  
    rpki::sql::sql\_persistent, 504  
sql\_encode  
    rpki::sql::sql\_persistent, 501  
sql\_fetch  
    rpki::sql::sql\_persistent, 501

sql\_fetch\_all  
    rpki::sql::sql\_persistent, 502  
sql\_fetch\_hook  
    rpki::rpki\_engine::roa\_obj, 482  
    rpki::sql::sql\_persistent, 502  
sql\_fetch\_where  
    rpki::sql::sql\_persistent, 502  
sql\_fetch\_where1  
    rpki::sql::sql\_persistent, 502  
sql\_in\_db  
    rpki::sql::sql\_persistent, 505  
sql\_init  
    rpki::sql::sql\_persistent, 502  
sql\_insert\_hook  
    rpki::rpki\_engine::roa\_obj, 482  
    rpki::sql::sql\_persistent, 503  
sql\_is\_dirty  
    rpki::sql::sql\_persistent, 503  
sql\_mark\_clean  
    rpki::sql::sql\_persistent, 503  
sql\_mark\_deleted  
    rpki::sql::sql\_persistent, 503  
sql\_mark\_dirty  
    rpki::sql::sql\_persistent, 503  
sql\_store  
    rpki::sql::sql\_persistent, 504  
sql\_template  
    rpki::left\_right::bsc\_elt, 300  
    rpki::left\_right::child\_elt, 305  
    rpki::left\_right::parent\_elt, 333  
    rpki::left\_right::repository\_elt, 342  
    rpki::left\_right::self\_elt, 352  
    rpki::publication::client\_elt, 366  
    rpki::publication::config\_elt, 373  
    rpki::rpki\_engine::ca\_detail\_obj,  
        459  
    rpki::rpki\_engine::ca\_obj, 466  
    rpki::rpki\_engine::child\_cert\_obj,  
        471  
    rpki::rpki\_engine::revoked\_cert\_obj,  
        477  
    rpki::rpki\_engine::roa\_obj, 484  
sql\_update\_hook  
    rpki::sql::sql\_persistent, 504  
stack  
    rpki::xml\_utils::sax\_handler, 633  
start  
    rpki::https::http\_client, 257  
start\_cron  
    rpki::rpki\_engine::rpkid\_context,  
        489  
startElement  
    rpki::left\_right::list\_resources\_elt,  
        321  
    rpki::left\_right::list\_roa\_requests\_-  
        elt, 324  
    rpki::publication::config\_elt, 372  
    rpki::up\_down::base\_elt, 522  
    rpki::up\_down::certificate\_elt, 524  
    rpki::up\_down::class\_elt, 528  
    rpki::up\_down::class\_response\_-  
        syntax, 531  
    rpki::up\_down::issue\_pdu, 540  
    rpki::up\_down::message\_pdu, 551  
    rpki::up\_down::revoke\_syntax, 561  
    rpki::xml\_utils::base\_elt, 619  
    rpki::xml\_utils::msg, 629  
    rpki::xml\_utils::sax\_handler, 632  
startElementNS  
    rpki::xml\_utils::sax\_handler, 633  
startup\_msg  
    irdbd, 58  
state  
    rpki::https::http\_client, 259  
    rpki::rpki\_engine::ca\_detail\_obj,  
        459  
status  
    rpki::up\_down::error\_response\_pdu,  
        537  
suggested\_sia\_head  
    rpki::up\_down::class\_elt, 529  
sundial.py(3191), 652  
supported\_address\_families  
    rpki::https, 79  
sweep  
    rpki::sql::session, 496  
symmetric\_difference  
    rpki::resource\_set::resource\_set, 417  
ta  
    rpki::https::http\_client, 259  
    rpki::https::http\_listener, 262

rpki::https::http\_queue, 270  
table rpki::sql::template, 508  
tag rpki::left\_right::report\_error\_elt, 337  
rpki::log, 85  
rpki::publication::report\_error\_elt, 393  
test rpki::sundial, 96  
test1 rpki::resource\_set, 92  
test2 rpki::resource\_set, 92  
text rpki::xml\_utils::sax\_handler, 633  
text\_attribute rpki::left\_right::list\_published\_objects\_elt, 316  
rpki::left\_right::report\_error\_elt, 337  
rpki::publication::report\_error\_elt, 393  
rpki::xml\_utils::text\_elt, 635  
textwrap::TextWrapper, 636  
thisUpdate rpki::manifest::Manifest, 360  
threshold rpki::async::gc\_summary, 171  
timeout rpki::https::http\_client, 259  
rpki::https::http\_server, 281  
timer rpki::async::gc\_summary, 171  
rpki::https::http\_stream, 289  
tls rpki::https::http\_client, 259  
rpki::https::http\_server, 281  
rpki::https::http\_stream, 290  
tls\_accept rpki::https::http\_server, 279  
tls\_connect rpki::https::http\_client, 257  
to\_bytes rpki::ipaddrs::v4addr, 291  
rpki::ipaddrs::v6addr, 294  
to\_DER rpki::x509::PEM\_converter, 588  
to\_PEM rpki::x509::PEM\_converter, 588  
to\_resource\_bag rpki::up\_down::class\_elt, 528  
to\_resource\_range rpki::resource\_set::roa\_prefix, 430  
to\_resource\_set rpki::resource\_set::roa\_prefix\_set, 437  
to\_rfc3779\_tuple rpki::resource\_set::resource\_range\_as, 405  
rpki::resource\_set::resource\_range\_ip, 408  
rpki::resource\_set::resource\_set\_as, 419  
rpki::resource\_set::resource\_set\_ip, 422  
to\_roa\_tuple rpki::resource\_set::roa\_prefix, 430  
rpki::resource\_set::roa\_prefix\_set, 438  
to\_sql rpki::sundial::datetime, 512  
rpki::x509::DER\_object, 585  
toASN1tuple rpki::sundial::datetime, 513  
toGeneralizedTime rpki::sundial::datetime, 513  
top\_opts irbe\_cli, 53  
totimestamp rpki::sundial::datetime, 513  
toUTCTime rpki::sundial::datetime, 513  
toXML rpki::left\_right::list\_resources\_elt, 321  
rpki::publication::publication\_object\_elt, 388  
rpki::up\_down::certificate\_elt, 524  
rpki::up\_down::class\_elt, 528  
rpki::up\_down::class\_response\_syntax, 531

rpki::up\_down::error\_response\_pdu, 537  
rpki::up\_down::issue\_pdu, 541  
rpki::up\_down::list\_pdu, 546  
rpki::up\_down::message\_pdu, 551  
rpki::up\_down::revoke\_syntax, 561  
rpki::xml\_utils::base\_elt, 620  
rpki::xml\_utils::data\_elt, 626  
rpki::xml\_utils::msg, 629  
rpki::xml\_utils::text\_elt, 635  
toXMLtime  
    rpki::sundial::datetime, 513  
trace  
    rpki::async::timer, 183  
    rpki::log, 84  
traceback  
    rpki::log, 84  
type  
    rpki::up\_down::message\_pdu, 552  
    rpki::xml\_utils::msg, 629  
type2name  
    rootd::message\_pdu, 166  
    rpki::up\_down::message\_pdu, 552

u

    irdbd, 58

undersized  
    rpki::resource\_set::resource\_bag, 400

unimplemented\_control  
    rpki::xml\_utils::data\_elt, 626

union  
    rpki::resource\_set::resource\_bag, 401  
    rpki::resource\_set::resource\_set, 417

unwind\_stack  
    rpki::async::iterator, 175

unwrap  
    rpki::x509::XML\_CMS\_object, 615

up\_down  
    rpki::relaxng, 89

up\_down.py(3162), 652

up\_down\_handler  
    rootd, 63  
    rpki::rpki\_engine::rpkid\_context, 490

    up\_down\_url\_regexp  
        rpki::rpki\_engine::rpkid\_context, 492

update  
    rpki::rpki\_engine::ca\_detail\_obj, 456  
    rpki::rpki\_engine::roa\_obj, 483  
    rpki::sql::template, 508

update\_children  
    rpki::left\_right::self\_elt, 350

update\_roas  
    rpki::left\_right::self\_elt, 351

update\_timeout  
    rpki::https::http\_stream, 288

uri  
    rpki::rpki\_engine::child\_cert\_obj, 469  
    rpki::rpki\_engine::roa\_obj, 483

uri\_tail  
    rpki::rpki\_engine::child\_cert\_obj, 470  
    rpki::rpki\_engine::roa\_obj, 483

uri\_to\_filename  
    rpki::publication::publication\_object\_elt, 388

uris  
    rpki::rpki\_engine::publication\_queue, 474

url  
    rpki::https::caller, 253

usage  
    irbe\_cli, 52  
    irbe\_cli::cmd\_elt\_mixin, 115  
    irbe\_cli::cmd\_msg\_mixin, 118

usage\_fill  
    irbe\_cli, 54

use\_hsm  
    rpki::left\_right::self\_elt, 353

use\_internal\_cron  
    rpki::rpki\_engine::rpkid\_context, 492

use\_syslog  
    rpki::log, 85

username  
    rpki::sql::session, 497

v4  
    rpki::resource\_set::resource\_bag,  
        401  
v6  
    rpki::resource\_set::resource\_bag,  
        401  
valid\_until  
    rpki::left\_right::list\_resources\_elt,  
        322  
    rpki::resource\_set::resource\_bag,  
        401  
verbose  
    irbe\_cli, 54  
verify  
    rpki::x509::CMS\_object, 568  
version  
    rpki::https::http\_message, 266  
    rpki::left\_right::msg, 327  
    rpki::left\_right::sax\_handler, 344  
    rpki::manifest::Manifest, 360  
    rpki::publication::msg, 382  
    rpki::publication::sax\_handler, 397  
    rpki::roa::RouteOriginAttestation,  
        449  
    rpki::up\_down::message\_pdu, 553  
    rpki::up\_down::sax\_handler, 564  
    rpki::xml\_utils::msg, 629

want\_persistent\_client  
    rpki::https, 79  
want\_persistent\_server  
    rpki::https, 79  
warn  
    rpki::log, 85  
when  
    rpki::async::timer, 184  
wired\_in\_config\_id  
    rpki::publication::config\_elt, 373  
withdraw  
    rpki::rpki\_engine::publication\_-  
        queue, 474  
wrap  
    rpki::x509::XML\_CMS\_object, 615  
writeable  
    rpki::https::http\_stream, 288