

RPKI Engine

1.0

Generated by Doxygen 1.7.3

Mon Jun 6 2011 15:44:39

Contents

1	RPKI Engine Reference Manual	1
2	Overview	2
2.1	Terminology	2
2.2	Programs	3
2.2.1	rpkid	4
2.2.2	pubd	5
2.2.3	rootd	5
2.2.4	irdbd	5
2.2.5	smoketest	6
2.2.6	yamltest	6
2.3	Further Reading	6
2.4	Getting Started	7
3	Installation Guide	7
4	Configuration Guide	10
4.1	rpki.conf	10
4.2	Other configuration files and options	14
4.3	Common Configuration Options	15
4.4	rpkid.conf	16
4.5	irdbd.conf	17
4.6	pubd.conf	18
4.7	rootd.conf	19
4.8	smoketest.conf	21
4.9	smoketest.yaml	21
5	MySQL Setup	23
6	The myrpki tool	24
6.1	myrpki overview	26
6.2	Hosted case	28
6.3	Self-hosted case	29
6.4	Hosting case	30
6.5	"Pure" hosting case	30
6.6	Troubleshooting	30
6.7	Known Issues	31
7	Left-Right Protocol	32
7.1	initiated by the IRBE	32
7.1.1	<self/> object	32
7.1.2	<bsc/> object	34
7.1.3	<parent/> object	35
7.1.4	<child/> object	37
7.1.5	<repository/> object	38

7.1.6	<route_origin/> object	38
7.2	Operations initiated by the RPKI engine	40
7.2.1	<list_resources/> messages	40
7.3	Error handling	41
8	Publication protocol	41
8.1	Publication control subprotocol	42
8.1.1	<config/> object	42
8.1.2	<client/> object	42
8.2	Publication subprotocol	43
8.2.1	<certificate/> object	43
8.2.2	<crl/> object	43
8.2.3	<manifest/> object	43
8.2.4	<roa/> object	44
8.3	Error handling	44
8.4	Additional access control considerations.	44
9	SQL database schemas	45
9.1	rpkid SQL schema	47
9.2	pubd SQL Schema	52
9.3	irdbd SQL Schema	53
10	BPKI model	55
11	Todo List	58
12	Namespace Documentation	58
12.1	Package irbe_cli	58
12.1.1	Detailed Description	59
12.1.2	Function Documentation	60
12.1.3	Variable Documentation	60
12.2	Package irdbd	63
12.2.1	Detailed Description	63
12.3	Package pubd	63
12.3.1	Detailed Description	63
12.4	Package rootd	64
12.4.1	Detailed Description	64
12.5	Package rpki	64
12.6	Package rpki.__doc__	65
12.7	Package rpki.adns	65
12.7.1	Detailed Description	65
12.7.2	Variable Documentation	66
12.8	Package rpki.async	66
12.8.1	Detailed Description	67
12.8.2	Function Documentation	67
12.8.3	Variable Documentation	68

12.9	Package rpki.cli	69
12.9.1	Detailed Description	69
12.9.2	Function Documentation	69
12.9.3	Variable Documentation	70
12.10	Package rpki.config	70
12.10.1	Detailed Description	70
12.10.2	Variable Documentation	71
12.11	Package rpki.exceptions	72
12.11.1	Detailed Description	73
12.12	Package rpki.http	74
12.12.1	Detailed Description	75
12.12.2	Function Documentation	76
12.12.3	Variable Documentation	77
12.13	Package rpki.ipaddrs	80
12.13.1	Detailed Description	80
12.13.2	Function Documentation	81
12.14	Package rpki.irdbd	81
12.14.1	Detailed Description	81
12.15	Package rpki.left_right	82
12.15.1	Detailed Description	82
12.15.2	Variable Documentation	83
12.16	Package rpki.log	83
12.16.1	Detailed Description	84
12.16.2	Function Documentation	85
12.16.3	Variable Documentation	86
12.17	Package rpki.manifest	87
12.17.1	Detailed Description	87
12.18	Package rpki.myrpki	88
12.18.1	Detailed Description	89
12.18.2	Function Documentation	90
12.18.3	Variable Documentation	91
12.19	Package rpki.oids	92
12.19.1	Detailed Description	92
12.19.2	Variable Documentation	93
12.20	Package rpki.pubd	93
12.20.1	Detailed Description	93
12.21	Package rpki.publication	94
12.21.1	Detailed Description	95
12.22	Package rpki.relaxng	95
12.22.1	Variable Documentation	96
12.23	Package rpki.resource_set	96
12.23.1	Detailed Description	97
12.23.2	Function Documentation	98
12.23.3	Variable Documentation	99
12.24	Package rpki.roa	100
12.24.1	Detailed Description	100

12.25	Package rpki.rootd	101
12.25.1	Detailed Description	101
12.25.2	Variable Documentation	102
12.26	Package rpki.rpkid	102
12.26.1	Detailed Description	103
12.27	Package rpki.sql	103
12.27.1	Detailed Description	103
12.28	Package rpki.sundial	104
12.28.1	Detailed Description	104
12.28.2	Function Documentation	105
12.29	Package rpki.up_down	106
12.29.1	Detailed Description	106
12.29.2	Variable Documentation	107
12.30	Package rpki.x509	107
12.30.1	Detailed Description	108
12.30.2	Function Documentation	109
12.31	Package rpki.xml_utils	110
12.31.1	Detailed Description	110
12.32	Package rpkid	110
12.32.1	Detailed Description	110
13	Class Documentation	111
13.1	async_chat Class Reference	111
13.2	dispatcher Class Reference	111
13.3	Cmd Class Reference	111
13.4	dict Class Reference	111
13.5	Exception Class Reference	112
13.6	irbe_cli.bsc_elt Class Reference	112
13.6.1	Detailed Description	112
13.6.2	Member Function Documentation	112
13.6.3	Member Data Documentation	113
13.7	irbe_cli.certificate_elt Class Reference	114
13.7.1	Detailed Description	114
13.8	irbe_cli.child_elt Class Reference	114
13.8.1	Detailed Description	114
13.9	irbe_cli.client_elt Class Reference	114
13.9.1	Detailed Description	114
13.10	irbe_cli.cmd_elt_mixin Class Reference	115
13.10.1	Detailed Description	115
13.10.2	Member Function Documentation	115
13.10.3	Member Data Documentation	116
13.11	irbe_cli.cmd_msg_mixin Class Reference	117
13.11.1	Detailed Description	118
13.11.2	Member Function Documentation	118
13.12	irbe_cli.config_elt Class Reference	118
13.12.1	Detailed Description	118

13.12.2 Member Function Documentation	119
13.12.3 Member Data Documentation	119
13.13irbe_cli.crl_elt Class Reference	119
13.13.1 Detailed Description	119
13.14irbe_cli.left_right_cms_msg Class Reference	119
13.14.1 Detailed Description	120
13.14.2 Member Data Documentation	120
13.15irbe_cli.left_right_msg Class Reference	120
13.15.1 Detailed Description	120
13.15.2 Member Data Documentation	120
13.16irbe_cli.left_right_proto Class Reference	121
13.16.1 Detailed Description	121
13.16.2 Member Data Documentation	121
13.17irbe_cli.left_right_sax_handler Class Reference	122
13.17.1 Detailed Description	122
13.17.2 Member Data Documentation	122
13.18irbe_cli.list_published_objects_elt Class Reference	122
13.18.1 Detailed Description	122
13.18.2 Member Data Documentation	123
13.19irbe_cli.list_received_resources_elt Class Reference	123
13.19.1 Detailed Description	123
13.19.2 Member Data Documentation	123
13.20irbe_cli.manifest_elt Class Reference	124
13.20.1 Detailed Description	124
13.21irbe_cli.parent_elt Class Reference	124
13.21.1 Detailed Description	124
13.22irbe_cli.publication_cms_msg Class Reference	124
13.22.1 Detailed Description	125
13.22.2 Member Data Documentation	125
13.23irbe_cli.publication_msg Class Reference	125
13.23.1 Detailed Description	125
13.23.2 Member Data Documentation	125
13.24irbe_cli.publication_proto Class Reference	126
13.24.1 Detailed Description	126
13.24.2 Member Data Documentation	126
13.25irbe_cli.publication_sax_handler Class Reference	127
13.25.1 Detailed Description	127
13.25.2 Member Data Documentation	127
13.26irbe_cli.reply_elt_mixin Class Reference	127
13.26.1 Detailed Description	128
13.26.2 Member Function Documentation	128
13.26.3 Member Data Documentation	128
13.27irbe_cli.report_error_elt Class Reference	128
13.27.1 Detailed Description	128
13.28irbe_cli.repository_elt Class Reference	129
13.28.1 Detailed Description	129

13.29	irbe_cli.roa_elt Class Reference	129
13.29.1	Detailed Description	129
13.30	irbe_cli.self_elt Class Reference	129
13.30.1	Detailed Description	129
13.31	irbe_cli.UsageWrapper Class Reference	130
13.31.1	Detailed Description	130
13.31.2	Member Function Documentation	130
13.32	long Class Reference	130
13.33	object Class Reference	130
13.34	datetime Class Reference	131
13.35	timedelta Class Reference	131
13.36	rpki.adns.dispatcher Class Reference	131
13.36.1	Detailed Description	131
13.36.2	Constructor & Destructor Documentation	132
13.36.3	Member Function Documentation	132
13.36.4	Member Data Documentation	133
13.37	rpki.adns.getaddrinfo Class Reference	133
13.37.1	Detailed Description	134
13.37.2	Constructor & Destructor Documentation	134
13.37.3	Member Function Documentation	134
13.37.4	Member Data Documentation	135
13.38	rpki.adns.query Class Reference	136
13.38.1	Detailed Description	136
13.38.2	Constructor & Destructor Documentation	137
13.38.3	Member Function Documentation	137
13.38.4	Member Data Documentation	139
13.39	rpki.adns.test_getaddrinfo Class Reference	141
13.39.1	Detailed Description	141
13.39.2	Constructor & Destructor Documentation	141
13.39.3	Member Function Documentation	141
13.39.4	Member Data Documentation	142
13.40	rpki.adns.test_query Class Reference	142
13.40.1	Detailed Description	142
13.40.2	Constructor & Destructor Documentation	143
13.40.3	Member Function Documentation	143
13.40.4	Member Data Documentation	143
13.41	rpki.async.gc_summary Class Reference	144
13.41.1	Detailed Description	144
13.41.2	Constructor & Destructor Documentation	144
13.41.3	Member Function Documentation	144
13.41.4	Member Data Documentation	145
13.42	rpki.async.iterator Class Reference	145
13.42.1	Detailed Description	146
13.42.2	Constructor & Destructor Documentation	146
13.42.3	Member Function Documentation	146
13.42.4	Member Data Documentation	147

13.43rpki.async.sync_wrapper Class Reference	147
13.43.1 Detailed Description	148
13.43.2 Constructor & Destructor Documentation	148
13.43.3 Member Function Documentation	148
13.43.4 Member Data Documentation	149
13.44rpki.async.timer Class Reference	150
13.44.1 Detailed Description	151
13.44.2 Constructor & Destructor Documentation	151
13.44.3 Member Function Documentation	151
13.44.4 Member Data Documentation	154
13.45rpki.cli.Cmd Class Reference	155
13.45.1 Detailed Description	155
13.45.2 Constructor & Destructor Documentation	156
13.45.3 Member Function Documentation	156
13.45.4 Member Data Documentation	158
13.46rpki.config.parser Class Reference	159
13.46.1 Detailed Description	159
13.46.2 Constructor & Destructor Documentation	160
13.46.3 Member Function Documentation	160
13.46.4 Member Data Documentation	162
13.47rpki.exceptions.BadClassNameSyntax Class Reference	162
13.47.1 Detailed Description	163
13.48rpki.exceptions.BadClientURL Class Reference	163
13.48.1 Detailed Description	163
13.49rpki.exceptions.BadContactURL Class Reference	163
13.49.1 Detailed Description	163
13.50rpki.exceptions.BadExtension Class Reference	164
13.50.1 Detailed Description	164
13.51rpki.exceptions.BadIPResource Class Reference	164
13.51.1 Detailed Description	164
13.52rpki.exceptions.BadIRDBReply Class Reference	164
13.52.1 Detailed Description	164
13.53rpki.exceptions.BadIssueResponse Class Reference	165
13.53.1 Detailed Description	165
13.54rpki.exceptions.BadPKCS10 Class Reference	165
13.54.1 Detailed Description	165
13.55rpki.exceptions.BadPublicationReply Class Reference	165
13.55.1 Detailed Description	165
13.56rpki.exceptions.BadQuery Class Reference	166
13.56.1 Detailed Description	166
13.57rpki.exceptions.BadROAPrefix Class Reference	166
13.57.1 Detailed Description	166
13.58rpki.exceptions.BadSender Class Reference	166
13.58.1 Detailed Description	167
13.59rpki.exceptions.BadStatusCode Class Reference	167
13.59.1 Detailed Description	167

13.60rpki.exceptions.BadURISyntax Class Reference	167
13.60.1 Detailed Description	167
13.61rpki.exceptions.BSCNotFound Class Reference	168
13.61.1 Detailed Description	168
13.62rpki.exceptions.BSCNotReady Class Reference	168
13.62.1 Detailed Description	168
13.63rpki.exceptions.ChildNotFound Class Reference	168
13.63.1 Detailed Description	168
13.64rpki.exceptions.ClassNameMismatch Class Reference	169
13.64.1 Detailed Description	169
13.65rpki.exceptions.ClassNameUnknown Class Reference	169
13.65.1 Detailed Description	169
13.66rpki.exceptions.ClientNotFound Class Reference	169
13.66.1 Detailed Description	169
13.67rpki.exceptions.CMSContentNotSet Class Reference	170
13.67.1 Detailed Description	170
13.68rpki.exceptions.CMSCRLNotSet Class Reference	170
13.68.1 Detailed Description	170
13.69rpki.exceptions.CMSVerificationFailed Class Reference	170
13.69.1 Detailed Description	171
13.70rpki.exceptions.CommandParseFailure Class Reference	171
13.70.1 Detailed Description	171
13.71rpki.exceptions.DBConsistencyError Class Reference	171
13.71.1 Detailed Description	171
13.72rpki.exceptions.DERObjectConversionError Class Reference	172
13.72.1 Detailed Description	172
13.73rpki.exceptions.DuplicateObject Class Reference	172
13.73.1 Detailed Description	172
13.74rpki.exceptions.EmptyPEM Class Reference	172
13.74.1 Detailed Description	172
13.75rpki.exceptions.EmptyROAPrefixList Class Reference	173
13.75.1 Detailed Description	173
13.76rpki.exceptions.ForbiddenURI Class Reference	173
13.76.1 Detailed Description	173
13.77rpki.exceptions.HandleTranslationError Class Reference	173
13.77.1 Detailed Description	173
13.78rpki.exceptions.HTTPBadVersion Class Reference	174
13.78.1 Detailed Description	174
13.79rpki.exceptions.HTTPClientAborted Class Reference	174
13.79.1 Detailed Description	174
13.80rpki.exceptions.HTTPRequestFailed Class Reference	174
13.80.1 Detailed Description	175
13.81rpki.exceptions.HTTPTimeout Class Reference	175
13.81.1 Detailed Description	175
13.82rpki.exceptions.HTTPUnexpectedState Class Reference	175
13.82.1 Detailed Description	175

13.83rpki.exceptions.MissingCMSCRL Class Reference	176
13.83.1 Detailed Description	176
13.84rpki.exceptions.MissingCMSEECert Class Reference	176
13.84.1 Detailed Description	176
13.85rpki.exceptions.MultipleTLSEECert Class Reference	176
13.85.1 Detailed Description	176
13.86rpki.exceptions.MustBePrefix Class Reference	177
13.86.1 Detailed Description	177
13.87rpki.exceptions.NoActiveCA Class Reference	177
13.87.1 Detailed Description	177
13.88rpki.exceptions.NoCoveringCertForROA Class Reference	177
13.88.1 Detailed Description	177
13.89rpki.exceptions.NoObjectAtURI Class Reference	178
13.89.1 Detailed Description	178
13.90rpki.exceptions.NotACertificateChain Class Reference	178
13.90.1 Detailed Description	178
13.91rpki.exceptions.NotFound Class Reference	178
13.91.1 Detailed Description	179
13.92rpki.exceptions.NotImplementedYet Class Reference	179
13.92.1 Detailed Description	179
13.93rpki.exceptions.NotInDatabase Class Reference	179
13.93.1 Detailed Description	179
13.94rpki.exceptions.ReceivedTLSCACert Class Reference	180
13.94.1 Detailed Description	180
13.95rpki.exceptions.RPKI_Exception Class Reference	180
13.95.1 Detailed Description	180
13.96rpki.exceptions.ServerShuttingDown Class Reference	181
13.96.1 Detailed Description	181
13.97rpki.exceptions.SKIMismatch Class Reference	181
13.97.1 Detailed Description	181
13.98rpki.exceptions.SubprocessError Class Reference	181
13.98.1 Detailed Description	182
13.99rpki.exceptions.TLSValidationError Class Reference	182
13.99.1 Detailed Description	182
13.100rpki.exceptions.UnexpectedCMSCerts Class Reference	182
13.100.1 Detailed Description	182
13.101rpki.exceptions.UnexpectedCMSCRLs Class Reference	183
13.101.1 Detailed Description	183
13.102rpki.exceptions.UnparsableCMSDER Class Reference	183
13.102.1 Detailed Description	183
13.103rpki.exceptions.UpstreamError Class Reference	183
13.103.1 Detailed Description	183
13.104rpki.exceptions.WrongContentType Class Reference	184
13.104.1 Detailed Description	184
13.105rpki.http.caller Class Reference	184
13.105.1 Detailed Description	185

13.105.2	Constructor & Destructor Documentation	185
13.105.3	Member Function Documentation	185
13.105.4	Member Data Documentation	185
13.106	pkhttp.http_client Class Reference	186
13.106.1	Detailed Description	187
13.106.2	Constructor & Destructor Documentation	187
13.106.3	Member Function Documentation	188
13.106.4	Member Data Documentation	190
13.107	pkhttp.http_listener Class Reference	191
13.107.1	Detailed Description	192
13.107.2	Constructor & Destructor Documentation	192
13.107.3	Member Function Documentation	192
13.107.4	Member Data Documentation	193
13.108	pkhttp.http_message Class Reference	193
13.108.1	Detailed Description	194
13.108.2	Constructor & Destructor Documentation	194
13.108.3	Member Function Documentation	194
13.108.4	Member Data Documentation	196
13.109	pkhttp.http_queue Class Reference	196
13.109.1	Detailed Description	197
13.109.2	Constructor & Destructor Documentation	197
13.109.3	Member Function Documentation	197
13.109.4	Member Data Documentation	199
13.110	pkhttp.http_request Class Reference	199
13.110.1	Detailed Description	200
13.110.2	Constructor & Destructor Documentation	200
13.110.3	Member Function Documentation	200
13.110.4	Member Data Documentation	201
13.111	pkhttp.http_response Class Reference	202
13.111.1	Detailed Description	202
13.111.2	Constructor & Destructor Documentation	202
13.111.3	Member Function Documentation	202
13.111.4	Member Data Documentation	203
13.112	pkhttp.http_server Class Reference	203
13.112.1	Detailed Description	204
13.112.2	Constructor & Destructor Documentation	204
13.112.3	Member Function Documentation	204
13.112.4	Member Data Documentation	206
13.113	pkhttp.http_stream Class Reference	206
13.113.1	Detailed Description	207
13.113.2	Constructor & Destructor Documentation	207
13.113.3	Member Function Documentation	208
13.113.4	Member Data Documentation	211
13.114	pkipaddr.v4addr Class Reference	212
13.114.1	Detailed Description	212
13.114.2	Member Function Documentation	212

13.114.3	Member Data Documentation	213
13.115	rpki.ipaddrs.v6addr Class Reference	213
13.115.1	Detailed Description	214
13.115.2	Member Function Documentation	214
13.115.3	Member Data Documentation	215
13.116	rpki.irdbd.main Class Reference	215
13.116.1	Detailed Description	215
13.116.2	Constructor & Destructor Documentation	216
13.116.3	Member Function Documentation	216
13.116.4	Member Data Documentation	216
13.117	rpki.left_right.bsc_elt Class Reference	218
13.117.1	Detailed Description	218
13.117.2	Member Function Documentation	219
13.117.3	Member Data Documentation	219
13.118	rpki.left_right.child_elt Class Reference	221
13.118.1	Detailed Description	222
13.118.2	Member Function Documentation	222
13.118.3	Member Data Documentation	224
13.119	rpki.left_right.cms_msg Class Reference	226
13.119.1	Detailed Description	226
13.119.2	Member Data Documentation	226
13.120	rpki.left_right.data_elt Class Reference	227
13.120.1	Detailed Description	227
13.120.2	Member Function Documentation	227
13.120.3	Member Data Documentation	229
13.121	rpki.left_right.left_right_namespace Class Reference	229
13.121.1	Detailed Description	230
13.121.2	Member Data Documentation	230
13.122	rpki.left_right.list_ghostbuster_requests_elt Class Reference	230
13.122.1	Detailed Description	231
13.122.2	Member Data Documentation	231
13.123	rpki.left_right.list_published_objects_elt Class Reference	232
13.123.1	Detailed Description	232
13.123.2	Member Function Documentation	232
13.123.3	Member Data Documentation	233
13.124	rpki.left_right.list_received_resources_elt Class Reference	234
13.124.1	Detailed Description	234
13.124.2	Member Function Documentation	234
13.124.3	Member Data Documentation	235
13.125	rpki.left_right.list_resources_elt Class Reference	235
13.125.1	Detailed Description	236
13.125.2	Member Function Documentation	236
13.125.3	Member Data Documentation	237
13.126	rpki.left_right.list_roa_requests_elt Class Reference	238
13.126.1	Detailed Description	238
13.126.2	Member Function Documentation	239

13.126.	Member Data Documentation	239
13.127.	rpki.left_right.msg Class Reference	240
13.127.	Detailed Description	240
13.127.	Member Function Documentation	240
13.127.	Member Data Documentation	240
13.128.	rpki.left_right.parent_elt Class Reference	241
13.128.	Detailed Description	242
13.128.	Member Function Documentation	242
13.128.	Member Data Documentation	244
13.129.	rpki.left_right.report_error_elt Class Reference	246
13.129.	Detailed Description	246
13.129.	Member Function Documentation	246
13.129.	Member Data Documentation	247
13.130.	rpki.left_right.repository_elt Class Reference	248
13.130.	Detailed Description	249
13.130.	Member Function Documentation	249
13.130.	Member Data Documentation	250
13.131.	rpki.left_right.sax_handler Class Reference	251
13.131.	Detailed Description	251
13.131.	Member Data Documentation	252
13.132.	rpki.left_right.self_elt Class Reference	252
13.132.	Detailed Description	253
13.132.	Member Function Documentation	254
13.132.	Member Data Documentation	258
13.133.	rpki.log.logger Class Reference	260
13.133.	Detailed Description	261
13.133.	Constructor & Destructor Documentation	261
13.133.	Member Function Documentation	261
13.133.	Member Data Documentation	261
13.134.	rpki.manifest.FileAndHash Class Reference	261
13.134.	Detailed Description	262
13.134.	Constructor & Destructor Documentation	262
13.134.	Member Data Documentation	262
13.135.	rpki.manifest.FilesAndHashes Class Reference	262
13.135.	Detailed Description	263
13.135.	Constructor & Destructor Documentation	263
13.136.	rpki.manifest.Manifest Class Reference	263
13.136.	Detailed Description	263
13.136.	Constructor & Destructor Documentation	264
13.136.	Member Data Documentation	264
13.137.	rpki.myrpki.CA Class Reference	265
13.137.	Detailed Description	266
13.137.	Constructor & Destructor Documentation	266
13.137.	Member Function Documentation	266
13.137.	Member Data Documentation	269
13.138.	rpki.myrpki.child Class Reference	271

13.138.	Detailed Description	271
13.138.	Constructor & Destructor Documentation	272
13.138.	Member Function Documentation	272
13.138.	Member Data Documentation	272
13.139.	rpki.myrpki.children Class Reference	274
13.139.	Detailed Description	274
13.139.	Member Function Documentation	274
13.140.	rpki.myrpki.comma_set Class Reference	275
13.140.	Detailed Description	275
13.140.	Member Function Documentation	275
13.141.	rpki.myrpki.csv_reader Class Reference	275
13.141.	Detailed Description	276
13.141.	Constructor & Destructor Documentation	276
13.141.	Member Function Documentation	276
13.141.	Member Data Documentation	277
13.142.	rpki.myrpki.csv_writer Class Reference	277
13.142.	Detailed Description	278
13.142.	Constructor & Destructor Documentation	278
13.142.	Member Function Documentation	278
13.142.	Member Data Documentation	279
13.143.	rpki.myrpki.EntityDB Class Reference	279
13.143.	Detailed Description	280
13.143.	Constructor & Destructor Documentation	280
13.143.	Member Function Documentation	280
13.143.	Member Data Documentation	280
13.144.	rpki.myrpki.IRDB Class Reference	281
13.144.	Detailed Description	281
13.144.	Constructor & Destructor Documentation	281
13.144.	Member Function Documentation	282
13.144.	Member Data Documentation	282
13.145.	rpki.myrpki.main Class Reference	283
13.145.	Detailed Description	284
13.145.	Constructor & Destructor Documentation	284
13.145.	Member Function Documentation	284
13.145.	Member Data Documentation	290
13.146.	rpki.myrpki.parent Class Reference	292
13.146.	Detailed Description	293
13.146.	Constructor & Destructor Documentation	293
13.146.	Member Function Documentation	293
13.146.	Member Data Documentation	293
13.147.	rpki.myrpki.parents Class Reference	294
13.147.	Detailed Description	294
13.147.	Member Function Documentation	295
13.148.	rpki.myrpki.repositories Class Reference	295
13.148.	Detailed Description	295
13.148.	Member Function Documentation	296

13.149.	rpki.myrpki.repository Class Reference	296
13.149.	Detailed Description	297
13.149.	Constructor & Destructor Documentation	297
13.149.	Member Function Documentation	297
13.149.	Member Data Documentation	298
13.150.	rpki.myrpki.roa_request Class Reference	298
13.150.	Detailed Description	299
13.150.	Constructor & Destructor Documentation	299
13.150.	Member Function Documentation	299
13.150.	Member Data Documentation	300
13.151.	rpki.myrpki.roa_requests Class Reference	301
13.151.	Detailed Description	301
13.151.	Member Function Documentation	301
13.152.	rpki.pubd.main Class Reference	302
13.152.	Detailed Description	302
13.152.	Constructor & Destructor Documentation	303
13.152.	Member Function Documentation	303
13.152.	Member Data Documentation	304
13.153.	rpki.publication.certificate_elt Class Reference	305
13.153.	Detailed Description	306
13.153.	Member Data Documentation	306
13.154.	rpki.publication.client_elt Class Reference	306
13.154.	Detailed Description	307
13.154.	Member Function Documentation	307
13.154.	Member Data Documentation	308
13.155.	rpki.publication.cms_msg Class Reference	309
13.155.	Detailed Description	309
13.155.	Member Data Documentation	309
13.156.	rpki.publication.config_elt Class Reference	310
13.156.	Detailed Description	311
13.156.	Member Function Documentation	311
13.156.	Member Data Documentation	312
13.157.	rpki.publication.control_elt Class Reference	313
13.157.	Detailed Description	313
13.157.	Member Function Documentation	313
13.158.	rpki.publication.crl_elt Class Reference	314
13.158.	Detailed Description	314
13.158.	Member Data Documentation	314
13.159.	rpki.publication.ghostbuster_elt Class Reference	315
13.159.	Detailed Description	315
13.159.	Member Data Documentation	315
13.160.	rpki.publication.manifest_elt Class Reference	315
13.160.	Detailed Description	316
13.160.	Member Data Documentation	316
13.161.	rpki.publication.msg Class Reference	316
13.161.	Detailed Description	317

13.161.2	Member Function Documentation	317
13.161.3	Member Data Documentation	317
13.162	pkf.publication.publication_namespace Class Reference	318
13.162.1	Detailed Description	318
13.162.2	Member Data Documentation	318
13.163	pkf.publication.publication_object_elt Class Reference	319
13.163.1	Detailed Description	319
13.163.2	Member Function Documentation	319
13.163.3	Member Data Documentation	321
13.164	pkf.publication.report_error_elt Class Reference	322
13.164.1	Detailed Description	323
13.164.2	Member Function Documentation	323
13.164.3	Member Data Documentation	323
13.165	pkf.publication.roa_elt Class Reference	325
13.165.1	Detailed Description	325
13.165.2	Member Data Documentation	325
13.166	pkf.publication.sax_handler Class Reference	325
13.166.1	Detailed Description	326
13.166.2	Member Data Documentation	326
13.167	pkf.resource_set.resource_bag Class Reference	326
13.167.1	Detailed Description	327
13.167.2	Constructor & Destructor Documentation	327
13.167.3	Member Function Documentation	328
13.167.4	Member Data Documentation	329
13.168	pkf.resource_set.resource_range Class Reference	330
13.168.1	Detailed Description	331
13.168.2	Constructor & Destructor Documentation	331
13.168.3	Member Function Documentation	331
13.168.4	Member Data Documentation	331
13.169	pkf.resource_set.resource_range_as Class Reference	332
13.169.1	Detailed Description	332
13.169.2	Member Function Documentation	332
13.169.3	Member Data Documentation	333
13.170	pkf.resource_set.resource_range_ip Class Reference	334
13.170.1	Detailed Description	334
13.170.2	Member Function Documentation	334
13.170.3	Member Data Documentation	336
13.171	pkf.resource_set.resource_range_ipv4 Class Reference	336
13.171.1	Detailed Description	336
13.171.2	Member Data Documentation	337
13.172	pkf.resource_set.resource_range_ipv6 Class Reference	337
13.172.1	Detailed Description	337
13.172.2	Member Data Documentation	337
13.173	pkf.resource_set.resource_set Class Reference	338
13.173.1	Detailed Description	338
13.173.2	Constructor & Destructor Documentation	339

13.173.	Member Function Documentation	339
13.173.	Member Data Documentation	342
13.174.	rpki.resource_set.resource_set_as Class Reference	342
13.174.	Detailed Description	343
13.174.	Member Function Documentation	343
13.174.	Member Data Documentation	343
13.175.	rpki.resource_set.resource_set_ip Class Reference	344
13.175.	Detailed Description	344
13.175.	Member Function Documentation	345
13.175.	Member Data Documentation	345
13.176.	rpki.resource_set.resource_set_ipv4 Class Reference	346
13.176.	Detailed Description	346
13.176.	Member Data Documentation	346
13.177.	rpki.resource_set.resource_set_ipv6 Class Reference	347
13.177.	Detailed Description	347
13.177.	Member Data Documentation	347
13.178.	rpki.resource_set.roa_prefix Class Reference	348
13.178.	Detailed Description	348
13.178.	Constructor & Destructor Documentation	349
13.178.	Member Function Documentation	349
13.178.	Member Data Documentation	350
13.179.	rpki.resource_set.roa_prefix_ipv4 Class Reference	351
13.179.	Detailed Description	351
13.179.	Member Data Documentation	351
13.180.	rpki.resource_set.roa_prefix_ipv6 Class Reference	352
13.180.	Detailed Description	352
13.180.	Member Data Documentation	352
13.181.	rpki.resource_set.roa_prefix_set Class Reference	352
13.181.	Detailed Description	353
13.181.	Constructor & Destructor Documentation	353
13.181.	Member Function Documentation	353
13.182.	rpki.resource_set.roa_prefix_set_ipv4 Class Reference	354
13.182.	Detailed Description	355
13.182.	Member Data Documentation	355
13.183.	rpki.resource_set.roa_prefix_set_ipv6 Class Reference	355
13.183.	Detailed Description	356
13.183.	Member Data Documentation	356
13.184.	rpki.roa.ROAIPAddress Class Reference	356
13.184.	Detailed Description	357
13.184.	Constructor & Destructor Documentation	357
13.184.	Member Data Documentation	357
13.185.	rpki.roa.ROAIPAddresses Class Reference	357
13.185.	Detailed Description	358
13.185.	Constructor & Destructor Documentation	358
13.186.	rpki.roa.ROAIPAddressFamilies Class Reference	358
13.186.	Detailed Description	358

13.186.	Constructor & Destructor Documentation	358
13.187.	rpki.roa.ROAIPAddressFamily Class Reference	359
13.187.	Detailed Description	359
13.187.	Constructor & Destructor Documentation	359
13.187.	Member Data Documentation	359
13.188.	rpki.roa.RouteOriginAttestation Class Reference	360
13.188.	Detailed Description	360
13.188.	Constructor & Destructor Documentation	360
13.188.	Member Data Documentation	361
13.189.	rpki.rootd.cms_msg Class Reference	361
13.189.	Detailed Description	361
13.189.	Member Data Documentation	362
13.190.	rpki.rootd.issue_pdu Class Reference	362
13.190.	Detailed Description	362
13.190.	Member Function Documentation	362
13.191.	rpki.rootd.list_pdu Class Reference	363
13.191.	Detailed Description	363
13.191.	Member Function Documentation	363
13.192.	rpki.rootd.main Class Reference	363
13.192.	Detailed Description	364
13.192.	Constructor & Destructor Documentation	365
13.192.	Member Function Documentation	365
13.192.	Member Data Documentation	366
13.193.	rpki.rootd.message_pdu Class Reference	369
13.193.	Detailed Description	370
13.193.	Member Function Documentation	370
13.193.	Member Data Documentation	370
13.194.	rpki.rootd.revoke_pdu Class Reference	371
13.194.	Detailed Description	371
13.194.	Member Function Documentation	371
13.195.	rpki.rootd.sax_handler Class Reference	372
13.195.	Detailed Description	372
13.195.	Member Data Documentation	372
13.196.	rpki.rpkid.ca_detail_obj Class Reference	372
13.196.	Detailed Description	373
13.196.	Member Function Documentation	374
13.196.	Member Data Documentation	379
13.197.	rpki.rpkid.ca_obj Class Reference	381
13.197.	Detailed Description	382
13.197.	Member Function Documentation	382
13.197.	Member Data Documentation	386
13.198.	rpki.rpkid.child_cert_obj Class Reference	387
13.198.	Detailed Description	388
13.198.	Constructor & Destructor Documentation	388
13.198.	Member Function Documentation	388
13.198.	Member Data Documentation	390

13.199	rpki.rpkid.ghostbuster_obj Class Reference	391
13.199.1	Detailed Description	392
13.199.2	Constructor & Destructor Documentation	392
13.199.3	Member Function Documentation	392
13.199.4	Member Data Documentation	395
13.200	rpki.rpkid.main Class Reference	396
13.200.1	Detailed Description	397
13.200.2	Constructor & Destructor Documentation	397
13.200.3	Member Function Documentation	398
13.200.4	Member Data Documentation	400
13.201	rpki.rpkid.publication_queue Class Reference	403
13.201.1	Detailed Description	403
13.201.2	Constructor & Destructor Documentation	404
13.201.3	Member Function Documentation	404
13.201.4	Member Data Documentation	404
13.202	rpki.rpkid.revoked_cert_obj Class Reference	405
13.202.1	Detailed Description	406
13.202.2	Constructor & Destructor Documentation	406
13.202.3	Member Function Documentation	406
13.202.4	Member Data Documentation	407
13.203	rpki.rpkid.roa_obj Class Reference	408
13.203.1	Detailed Description	409
13.203.2	Constructor & Destructor Documentation	409
13.203.3	Member Function Documentation	409
13.203.4	Member Data Documentation	412
13.204	rpki.sql.session Class Reference	414
13.204.1	Detailed Description	415
13.204.2	Constructor & Destructor Documentation	415
13.204.3	Member Function Documentation	415
13.204.4	Member Data Documentation	417
13.205	rpki.sql.sql_persistent Class Reference	418
13.205.1	Detailed Description	419
13.205.2	Member Function Documentation	419
13.205.3	Member Data Documentation	423
13.206	rpki.sql.template Class Reference	424
13.206.1	Detailed Description	424
13.206.2	Constructor & Destructor Documentation	424
13.206.3	Member Data Documentation	425
13.207	rpki.sundial.datetime Class Reference	426
13.207.1	Detailed Description	427
13.207.2	Member Function Documentation	427
13.207.3	Member Data Documentation	430
13.208	rpki.sundial.timedelta Class Reference	431
13.208.1	Detailed Description	431
13.208.2	Member Function Documentation	432
13.208.3	Member Data Documentation	434

13.209	rpki.up_down.base_elt Class Reference	435
13.209	Detailed Description	435
13.209	Member Function Documentation	435
13.210	rpki.up_down.certificate_elt Class Reference	437
13.210	Detailed Description	437
13.210	Member Function Documentation	438
13.210	Member Data Documentation	438
13.211	rpki.up_down.class_elt Class Reference	439
13.211	Detailed Description	440
13.211	Constructor & Destructor Documentation	440
13.211	Member Function Documentation	440
13.211	Member Data Documentation	441
13.212	rpki.up_down.class_response_syntax Class Reference	442
13.212	Detailed Description	443
13.212	Constructor & Destructor Documentation	443
13.212	Member Function Documentation	443
13.212	Member Data Documentation	444
13.213	rpki.up_down.cms_msg Class Reference	444
13.213	Detailed Description	444
13.213	Member Data Documentation	444
13.214	rpki.up_down.error_response_pdu Class Reference	445
13.214	Detailed Description	445
13.214	Constructor & Destructor Documentation	446
13.214	Member Function Documentation	446
13.214	Member Data Documentation	447
13.215	rpki.up_down.issue_pdu Class Reference	448
13.215	Detailed Description	448
13.215	Member Function Documentation	448
13.215	Member Data Documentation	449
13.216	rpki.up_down.issue_response_pdu Class Reference	450
13.216	Detailed Description	450
13.216	Member Function Documentation	451
13.217	rpki.up_down.list_pdu Class Reference	451
13.217	Detailed Description	451
13.217	Member Function Documentation	451
13.218	rpki.up_down.list_response_pdu Class Reference	452
13.218	Detailed Description	452
13.219	rpki.up_down.message_pdu Class Reference	452
13.219	Detailed Description	453
13.219	Member Function Documentation	453
13.219	Member Data Documentation	455
13.220	rpki.up_down.multi_uri Class Reference	456
13.220	Detailed Description	457
13.220	Constructor & Destructor Documentation	457
13.220	Member Function Documentation	457
13.221	rpki.up_down.revoke_pdu Class Reference	457

13.221.Detailed Description	458
13.221.2.Member Function Documentation	458
13.221.3.Member Data Documentation	459
13.222.Rpki.up_down.revoke_response_pdu Class Reference	459
13.222.Detailed Description	459
13.223.Rpki.up_down.revoke_syntax Class Reference	459
13.223.Detailed Description	460
13.223.2.Member Function Documentation	460
13.223.3.Member Data Documentation	461
13.224.Rpki.up_down.sax_handler Class Reference	461
13.224.Detailed Description	461
13.224.2.Member Data Documentation	461
13.225.Rpki.x509.CMS_object Class Reference	462
13.225.Detailed Description	463
13.225.2.Member Function Documentation	463
13.225.3.Member Data Documentation	465
13.226.Rpki.x509.CRL Class Reference	467
13.226.Detailed Description	468
13.226.2.Member Function Documentation	468
13.226.3.Member Data Documentation	470
13.227.Rpki.x509.DeadDrop Class Reference	471
13.227.Detailed Description	471
13.227.2.Constructor & Destructor Documentation	471
13.227.3.Member Function Documentation	472
13.227.4.Member Data Documentation	472
13.228.Rpki.x509.DER_CMS_object Class Reference	472
13.228.Detailed Description	472
13.228.2.Member Function Documentation	473
13.228.3.Member Data Documentation	473
13.229.Rpki.x509.DER_object Class Reference	473
13.229.Detailed Description	475
13.229.2.Constructor & Destructor Documentation	475
13.229.3.Member Function Documentation	475
13.229.4.Member Data Documentation	480
13.230.Rpki.x509.Ghostbuster Class Reference	481
13.230.Detailed Description	482
13.230.2.Member Function Documentation	482
13.230.3.Member Data Documentation	483
13.231.Rpki.x509.PEM_converter Class Reference	483
13.231.Detailed Description	484
13.231.2.Constructor & Destructor Documentation	484
13.231.3.Member Function Documentation	484
13.231.4.Member Data Documentation	485
13.232.Rpki.x509.PKCS10 Class Reference	485
13.232.Detailed Description	486
13.232.2.Member Function Documentation	486

13.232.3.Member Data Documentation	487
13.233.RPKI.x509.ROA Class Reference	488
13.233.1.Detailed Description	489
13.233.2.Member Function Documentation	489
13.233.3.Member Data Documentation	489
13.234.RPKI.x509.RSA Class Reference	490
13.234.1.Detailed Description	490
13.234.2.Member Function Documentation	491
13.234.3.Member Data Documentation	492
13.235.RPKI.x509.RSAPublic Class Reference	493
13.235.1.Detailed Description	493
13.235.2.Member Function Documentation	493
13.235.3.Member Data Documentation	494
13.236.RPKI.x509.SignedManifest Class Reference	495
13.236.1.Detailed Description	495
13.236.2.Member Function Documentation	496
13.236.3.Member Data Documentation	496
13.237.RPKI.x509.X509 Class Reference	497
13.237.1.Detailed Description	498
13.237.2.Member Function Documentation	498
13.237.3.Member Data Documentation	501
13.238.RPKI.x509.XML_CMS_object Class Reference	502
13.238.1.Detailed Description	502
13.238.2.Member Function Documentation	502
13.238.3.Member Data Documentation	504
13.239.RPKI.xml_utils.base_elt Class Reference	505
13.239.1.Detailed Description	505
13.239.2.Member Function Documentation	506
13.239.3.Member Data Documentation	507
13.240.RPKI.xml_utils.data_elt Class Reference	508
13.240.1.Detailed Description	509
13.240.2.Member Function Documentation	509
13.241.RPKI.xml_utils.msg Class Reference	512
13.241.1.Detailed Description	513
13.241.2.Member Function Documentation	513
13.241.3.Member Data Documentation	514
13.242.RPKI.xml_utils.sax_handler Class Reference	515
13.242.1.Detailed Description	515
13.242.2.Constructor & Destructor Documentation	516
13.242.3.Member Function Documentation	516
13.242.4.Member Data Documentation	517
13.243.RPKI.xml_utils.text_elt Class Reference	518
13.243.1.Detailed Description	518
13.243.2.Member Function Documentation	518
13.243.3.Member Data Documentation	519
13.244.Sequence Class Reference	519

13.24SequenceOf Class Reference	519
13.246et Class Reference	519
13.24TextWrapper Class Reference	520
13.24ContentHandler Class Reference	520
14 File Documentation	520
14.1 __doc__.py File Reference	520
14.1.1 Detailed Description	520
14.2 __init__.py File Reference	521
14.3 adns.py File Reference	521
14.4 async.py File Reference	522
14.5 cli.py File Reference	522
14.6 config.py File Reference	523
14.7 exceptions.py File Reference	523
14.8 http.py File Reference	525
14.9 ipaddrs.py File Reference	527
14.10irbe_cli.py File Reference	527
14.11irdbd.py File Reference	529
14.12irdbd.py File Reference	529
14.13left_right.py File Reference	529
14.14log.py File Reference	530
14.15manifest.py File Reference	531
14.16myrpkid.py File Reference	531
14.17oids.py File Reference	532
14.18pubd.py File Reference	532
14.19pubd.py File Reference	533
14.20publication.py File Reference	533
14.21relaxng.py File Reference	533
14.22resource_set.py File Reference	534
14.23roa.py File Reference	535
14.24rootd.py File Reference	535
14.25rootd.py File Reference	536
14.26rpkid.py File Reference	536
14.27rpkid.py File Reference	536
14.28sql.py File Reference	536
14.29sundial.py File Reference	537
14.30up_down.py File Reference	537
14.31x509.py File Reference	538
14.32xml_utils.py File Reference	539

1 RPKI Engine Reference Manual

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

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

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

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

The documentation you're reading is generated automatically by Doxygen from comments and documentation in [the code](#).

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

- [Overview of the tools](#)
- [Installation instructions](#)
- [Configuration instructions](#)
- [MySQL setup instructions](#)
- The [myrpki](#) tool
- A description of the [left-right](#) protocol
- A description of the [publication](#) protocol
- A description of the [BPKI model](#) used to secure the up-down, left-right, and publication protocols
- A description of the several [SQL database schemas](#)

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

2 Overview

2.1 Terminology

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

Todo

These explanations should be fleshed out properly.

IRBE:

Internet Registry Back End.

IRDB:

Internet Registry Data Base.

BPKI:

Business PKI.

RPKI:

Resource PKI.

2.2 Programs

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

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

- `rpkid`: The main RPKI engine daemon.
- `pubd`: The publication engine daemon.
- `rootd`: A separate daemon for handling the root of an RPKI certificate tree. This is essentially a stripped down version of `rpkid` with no SQL database, no left-right protocol implementation, and only the parent side of the up-down protocol. It's separate because the root is a special case in several ways and it was simpler to keep the special cases out of the main daemon.
- `irdbd`: A sample implementation of an IR database daemon. `rpkid` calls into this to perform lookups via the left-right protocol.
- `smoketest`: A test tool for running a collection of `rpkid` and `irdb` instances under common control, driven by a unified test script.
- `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.

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 of configuration files which may be useful as examples.

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

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

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

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

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

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

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

2.2.1 rpkid

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

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

2.2.2 pubd

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

pubd is separate from rpkid for two reasons:

- The hosting model allows entities which choose to run their own copies of rpkid to publish their output under a common publication point. In general, encouraging shared publication services where practical is a good thing for relying parties, as it will speed up rcynic synchronization time.
- The publication server has to run on (or at least close to) the publication point itself, which in turn must be on a publically reachable server to be useful. rpkid, on the other hand, need only be reachable by the IRBE and its children in the RPKI tree. rpkid is a much more complex piece of software than pubd, so in some situations it might make sense to wrap tighter firewall constraints around rpkid than would be practical if rpkid and pubd were a single program.

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

2.2.3 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; see the [Configuration Guide](#) for details.

2.2.4 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.

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

2.2.5 smoketest

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

Unlike the programs described above, smoketest takes two configuration files in different languages. The first configuration file uses the same syntax as the above configuration files but is completely optional. The second configuration file is the test script, which is encoded using the YAML serialization language (see <http://www.yaml.org/> for more information on YAML). The YAML script is not optional, as it describes the test layout. smoketest is designed to support running a fairly wide set of test configurations as canned scripts without writing any new control code. The intent is to make it possible to write meaningful regression tests.

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

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

2.2.6 yamlttest

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

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

2.3 Further Reading

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

- [The rcynic validation tool](#)
- [A live sample of rcynic's summary output](#)

2.4 Getting Started

The first step to bringing up rpkiid and friends is installing the code, which is described in the [Installation Guide](#).

3 Installation Guide

Installation instructions for rpkiid et al.

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

rpkiid is a set of Python modules supporting generation and maintenance of resource certificates. Most of the code is in the rpkiid/rpki/ directory. rpkiid 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. rpkiid 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. rpkiid 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, run the configure script, then run "make":

```
$ cd $top
$ ./configure
$ make
```

This should automatically build everything, in the right order, including 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 rpki/ 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 rpki/tests/smoketest.setup.sql. The MySQL command line client is usually the easiest way to do this, eg:

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

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

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

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

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

- <http://www.doxygen.org/>. Doxygen in turn pulls in several other tools, notably Graphviz, pdfLaTeX, and Ghostscript.
 - FreeBSD: /usr/ports/devel/doxygen
 - Ubuntu: doxygen
- <http://www.mbayer.de/html2text/>. The documentation build process uses xsltproc and html2text to dump flat text versions of a few critical documentation pages.
 - FreeBSD: /usr/ports/textproc/html2text
- <http://www.thaiopensource.com/relaxng/trang.html>. Trang is used to convert RelaxNG schemas from the human-readable "compact" form to the XML form that LibXML2 understands. Trang in turn requires Java.
 - FreeBSD: /usr/ports/textproc/trang
- <http://search.cpan.org/dist/SQL-Translator/>. SQL-Translator, also known as "SQL Fairy", includes code to parse an SQL schema and dump a description of it as Graphviz input. SQL Fairy in turn requires Perl.
 - FreeBSD: /usr/ports/databases/p5-SQL-Translator

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

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.

4.1 `rpki.conf`

The default name for the shared configuration file is `rpki.conf`. Unless you really know what you're doing, you should start by copying the `rpki.conf` from the `rpkid/examples` directory and modifying it, as the sample configuration file already includes all the additional settings necessary to use the simplified configuration.

```
[myrpki]
```

The `[myrpki]` section of `rpki.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 rpki'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 `rpki.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.

4.2 Other configuration files and options

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

- [Common configuration options](#)
- [rpkid configuration](#)
- [irdbd configuration](#)
- [pubd configuration](#)

- [rootd configuration](#)
- [configuration of the smoketest test harness](#)
- [test description language for the smoketest test harness](#)

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

4.3 Common Configuration Options

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

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

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

debug_http:

Enable verbose http debug logging.

debug_tls_certs:

Enable verbose logging about tls certs.

want_persistent_client:

Enable http 1.1 persistence, client side.

want_persistent_server:

Enable http 1.1 persistence, server side.

debug_cms_certs:

Enable verbose logging about cms certs.

sql_debug:

Enable verbose logging about sql operations.

gc_debug:

Enable scary garbage collector debugging.

timer_debug:

Enable verbose logging of timer system.

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

dump_outbound_cms:

Dump messages we send to this mailbox.

dump_inbound_cms:

Dump messages we receive to this mailbox.

4.4 rpkiid.conf

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

All options are in the section "[rpkiid]". 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 rpkiid instances at once.

sql-username:

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

sql-database:

MySQL's database name for rpkiid's database.

sql-password:

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

bpki-ta:

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

rpkiid-cert:

Name of file containing rpkiid'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 http:// URL.

server-host:

Hostname or IP address on which to listen for HTTP 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 HTTP connections.

4.5 irdbd.conf

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

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

Config file options:

startup-message:

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

sql-username:

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

sql-database:

MySQL's database name for irdbd's database.

sql-password:

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

bpki-ta:

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

irdbd-cert:

Name of file containing irdbd's own BPKI certificate.

irdbd-key:

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

rpkid-cert:

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

http-url:

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

4.6 pubd.conf

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

All options are in the section "[pubd]". 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.

bpki-ta:

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

irbe-cert:

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

pubd-cert:

Name of file containing BPKI certificate used by pubd.

pubd-key:

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

server-host:

Hostname or IP address on which to listen for HTTP 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 HTTP connections.

publication-base:

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

4.7 rootd.conf

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

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

Config file options:

bpki-ta:

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

rootd-bpki-cert:

Name of file containing rootd's own BPKI certificate.

rootd-bpki-key:

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

rootd-bpki-crl:

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

child-bpki-cert:

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

server-host:

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

server-port:

TCP port on which to listen for HTTP connections.

rpki-root-key:

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

rpki-root-cert:

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

rpki-root-dir:

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

rpki-subject-cert:

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

rpki-root-crl:

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

rpki-root-manifest:

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

rpki-subject-pkcs10:

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

4.8 smoketest.conf

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

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

4.9 smoketest.yaml

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

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

Here's an example of current usage:

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

This specifies an initial layout consisting of an RPKI engine named "Alice", with one child "Bob", which in turn has one child "Carol". Carol has a set of assigned resources,

and all resources in the system are initially set to be valid for two days from the time at which the test is started. The first subsequent document adds ten seconds to the validity interval for Carol's resources and makes no other modifications. The second subsequent document grants Carol additional resources and adds another two days to the validity interval for Carol's resources. The next document subtracts two days from the validity interval for Carol's resources. The final document sets the validity interval for Carol's resources to ten days.

Operators in subsequent (update) documents:

add_as:

Add ASN resources.

add_v4:

Add IPv4 resources.

add_v6:

Add IPv6 resources.

sub_as:

Subtract ASN resources.

sub_v4:

Subtract IPv4 resources.

sub_v6:

Subtract IPv6 resources.

valid_until:

Set an absolute expiration date.

valid_for:

Set a relative expiration date.

valid_add:

Add to validity interval.

valid_sub:

Subtract from validity interval.

sleep [interval]:

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

shell cmd...:

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

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

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

5 MySQL Setup

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

See the [Installation Guide](#) for details on where to download MySQL and find documentation on installing it.

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

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

Using the script is simple:

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

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

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

```
$ mysql -u root -p
```

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

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

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

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

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

Once you've finished configuring MySQL, the next thing you should read is the instructions for the [myrpki tool](#).

6 The myrpki tool

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

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

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

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

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

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

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

The basic idea here is that a user who has resources maintains a set of .csv files containing a text representation of the data needed by the back-end, along with a configuration file containing other parameters. The intent is that these be very simple files that are easy to generate either by hand or as a dump from relational database, spreadsheet, awk script, whatever works in your environment. Given these files, the user then runs `myrpki` to extract the relevant information and encode everything about its back end state into an XML file, which can then be shipped to the appropriate other party.

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

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

regenerate these expiring objects, but fixing this will be a relatively minor matter.]

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

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

Keep reading, and don't panic.

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

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

6.1 myrpki overview

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

"\$top" in the following refers to wherever you put the `subvert-rpki.hactrn.net` code. Once we have `autoconf` and "make install" targets, this will be some system directory or another; for now, it's wherever you checked out a copy of the code from the subversion repository or unpacked a tarball of the code.

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

The steps needed during setup phase are:

- Write a configuration file (copy `$top/rpkid/examples/rpki.conf` and edit as needed). You need to configure the `[myrpki]` section; in theory, the rest of the file should be ok as it is, at least for simple use. You also need to create (either by hand or by dumping from a database, spreadsheet, whatever) the CSV files describing prefixes and ASNs you want to allocate to your children and ROAs you want created.
- Initialization ("`initialize`" command). This creates the local BPKI and other data structures that can be constructed just based on local data such as the config

file. Other than some internal data structures, the main output of this step is the "identity.xml" file, which is used as input to later stages.

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

- Send (email, USB stick, carrier pigeon) identity.xml to each of your parents. This tells each of your parents what you call yourself, and supplies each parent with a trust anchor for your resource-holding BPKI.
- Each of your parents runs the "configure_child" command, giving the identity.xml you supplied as input. This registers your data with the parent, including BPKI cross-registration, and generates a return message containing your parent's BPKI trust anchors, a service URL for contacting your parent via the "up-down" protocol, and (usually) either an offer of publication service (if your parent operates a repository) or a referral from your parent to whatever publication service your parent does use. Referrals include a CMS-signed authorization token that the repository operator can use to determine that your parent has given you permission to home underneath your parent in the publication tree.
- Each of your parents sends (...) back the response XML file generated by the "configure_child" command.
- You feed the response message you just got into myrpki using the "configure_parent" command. This registers the parent's information in your database, including BPKI cross-certification, and processes the repository offer or referral to generate a publication request message.
- You send (...) the publication request message to the repository. The `contact_info` element in the request message should (in theory) provide some clue as to where you should send this.
- The repository operator processes your request using myrpki's "configure_publication_client" command. This registers your information, including BPKI cross-certification, and generates a response message containing the repository's BPKI trust anchor and service URL.
- Repository operator sends (...) the publication confirmation message back to you.
- You process the publication confirmation message using myrpki's "configure_repository" command.

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

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

6.2 Hosted case

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

- Run through steps listed in [the myrpki overview section](#).
- Run the configure_resources command to generate myrpki.xml.
- Send myrpki.xml to the rpki operator who will be hosting you.
- Wait for your rpki operator to ship you back an updated XML file containing a PKCS #10 certificate request for the BPKI signing context (BSC) created by rpki.
- Run configure_resources again with the XML file you just received, to issue the BSC certificate and update the XML file again to contain the newly issued BSC certificate.
- Send the updated XML file back to your rpki operator.

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

Warning

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

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

6.3 Self-hosted case

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

The [current] steps are:

- Follow the basic installation instructions in [the Installation Guide](#) to build the RFC-3779-aware OpenSSL code and associated Python extension module.
- Run through steps listed in [the myrpki overview section](#).
- Set up the MySQL databases that rpkid et al will use. The package includes a tool to do this for you, you can use that or do the job by hand. See [MySQL database setup](#) for details.
- If you are running your own publication repository (that is, if you are running pubd), you will also need to set up an rsyncd server or configure your existing one to serve pubd's output. There's a sample configuration file in \$top/rpkid/examples/rsyncd.conf, but you may need to do something more complicated if you are already running rsyncd for other purposes. See the rsync(1) and rsyncd.conf(5) manual pages for more details.
- Start the daemons. You can use \$top/rpkid/rpki-start-servers.py to do this, or write your own script. If you intend to run pubd, you should make sure that the directory you specified as publication_base_directory exists and is writable by the userid that will be running pubd, and should also make sure to start rsyncd.
- Run myrpki's configure_daemons command, twice, with no arguments. You need to run the command twice because myrpki has to ask rpkid to create a key-pair and generate a certification request for the BSC. The first pass does this, the second processes the certification request, issues the BSC, and loads the result into rpkid. [Yes, we could automate this somehow, if necessary.]

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

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

6.4 Hosting case

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

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

6.5 "Pure" hosting case

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

Todo

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

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

6.6 Troubleshooting

If you run into trouble setting up this package, the first thing to do is categorize the kind of trouble you are having. If you've gotten far enough to be running the daemons, check their log files. If you're seeing Python exceptions, read the error messages. If

you're getting TLS errors, check to make sure that you're using all the right BPKI certificates and service contact URLs.

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

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

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

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

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

6.7 Known Issues

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

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

not be needed here and would not be if not for this GNU linker issue.

7 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.

7.1 initiated by the IRBE

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

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

Left-right protocol objects are encoded as signed CMS messages containing XML as eContent and using an eContentType OID of `id-ct-xml` (1.2.840.113549.1.9.16.1.28). These CMS messages are in turn passed as the data for HTTP 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.

7.1.1 `<self/>` object

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

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

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

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

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

use_hsm (attribute):

Whether to use a Hardware Signing Module. At present this option has no effect, as the implementation does not yet support HSMs.

crl_interval (attribute):

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

regen_margin (attribute):

Positive integer representing how long before expiration of an RPKI certificate a new one should be generated, measured in seconds. At present this only affects the one-off EE certificates associated with ROAs. This parameter also controls how long before the nextUpdate time of CRL or manifest the CRL or manifest should be updated.

bpki_cert (element):

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

bpki_glue (element):

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

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

rekey:

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

revoke:

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

reissue:

Not implemented, may be removed from protocol. Original theory was that this operation would force reissuance of any object with a changed key, but as that happens automatically as part of the key rollover mechanism this operation seems unnecessary.

run_now:

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

publish_world_now:

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

7.1.2 `<bsc/>` object

The `<bsc/>` ("business signing context") object represents all the BPKI data needed to sign outgoing CMS 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.

7.1.3 `<parent/>` object

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

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

when signing messages sent to this parent, and a `repository_handle` indicating the `<repository/>` object to be used when publishing issued by the certificate issued by this parent.

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

peer_contact_uri (attribute):

HTTP 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.

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.

7.1.4 `<child/>` object

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

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

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

bpki_cert (element):

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

bpki_glue (element):

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

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

reissue:

Not implemented, may be removed from protocol.

7.1.5 <repository/> object

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

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

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

peer_contact_uri (attribute):

HTTP 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.

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

7.1.6 <route_origin/> object

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

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

Note that a <route_origin/> object represents a ROA to be generated on behalf of <self/>, not on behalf of a <child/>. Thus, a hosted entity that has no children but which does need to generate ROAs would be represented by a hosted

<self/> with no <child/> objects but one or more <route_origin/> objects. While lumping ROA generation in with the other RPKI engine activities may seem a little odd at first, it's a natural consequence of the design requirement that the RPKI daemon never transmit private keys across the network in any form; given this requirement, the RPKI engine that holds the private keys for an RPKI certificate must also be the engine which generates any ROAs that derive from that RPKI certificate.

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

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

asn (attribute):

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

ipv4 (attribute):

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

ipv6 (attribute):

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

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

suppress_publication:

Not implemented, may be removed from protocol.

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

ABNF for these address lists:

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

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

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

7.2 Operations initiated by the RPKI engine

The left-right protocol also includes queries from the RPKI engine back to the IRDB. These queries do not follow the message-passing pattern used in the IRBE-initiated part of the protocol. Instead, there's a single query back to the IRDB, with a corresponding response. The CMS 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.

7.2.1 `<list_resources/>` messages

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

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

valid_until:

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

asn:

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

ipv4:

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

ipv6:

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

Entries in a list of address prefixes and ranges can be either prefixes, which are written in the usual address/prefixlen notation, or ranges, which are expressed as a pair of addresses denoting the beginning and end of the range, written in ascending order separated by a single "-" character. This format is superficially similar to the format used

for prefix and maxLength values in the `<route_origin/>` object, but the semantics differ: note in particular that `<route_origin/>` objects don't allow ranges, while `<list_resources/>` messages don't allow a maxLength specification.

7.3 Error handling

Error in this protocol are handled at two levels.

Since all messages in this protocol are conveyed over HTTP 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.

8 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 HTTP with the same eContentType OID and the same HTTP 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 HTTP server which serves both of these subprotocols. The two subprotocols share a single server port, but use distinct URLs to allow demultiplexing.

8.1 Publication control subprotocol

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

8.1.1 <config/> object

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

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

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

bpki_crl (element):

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

8.1.2 <client/> object

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

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

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

base_uri (attribute):

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

bpki_cert (element):

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

bpki_glue (element):

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

8.2 Publication subprotocol

The publication subprotocol is structured somewhat differently from the publication control protocol. Objects in the publication subprotocol represent objects to be published or objects to be withdrawn from publication. Each kind of object supports two actions: "publish" and "withdraw". In each case the XML element representing 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.

8.2.1 <certificate/> object

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

8.2.2 <crl/> object

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

8.2.3 <manifest/> object

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

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

8.2.4 <roa/> object

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

8.3 Error handling

Error in this protocol are handled at two levels.

Since all messages in this protocol are conveyed over HTTP 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.

8.4 Additional access control considerations.

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

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

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

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

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

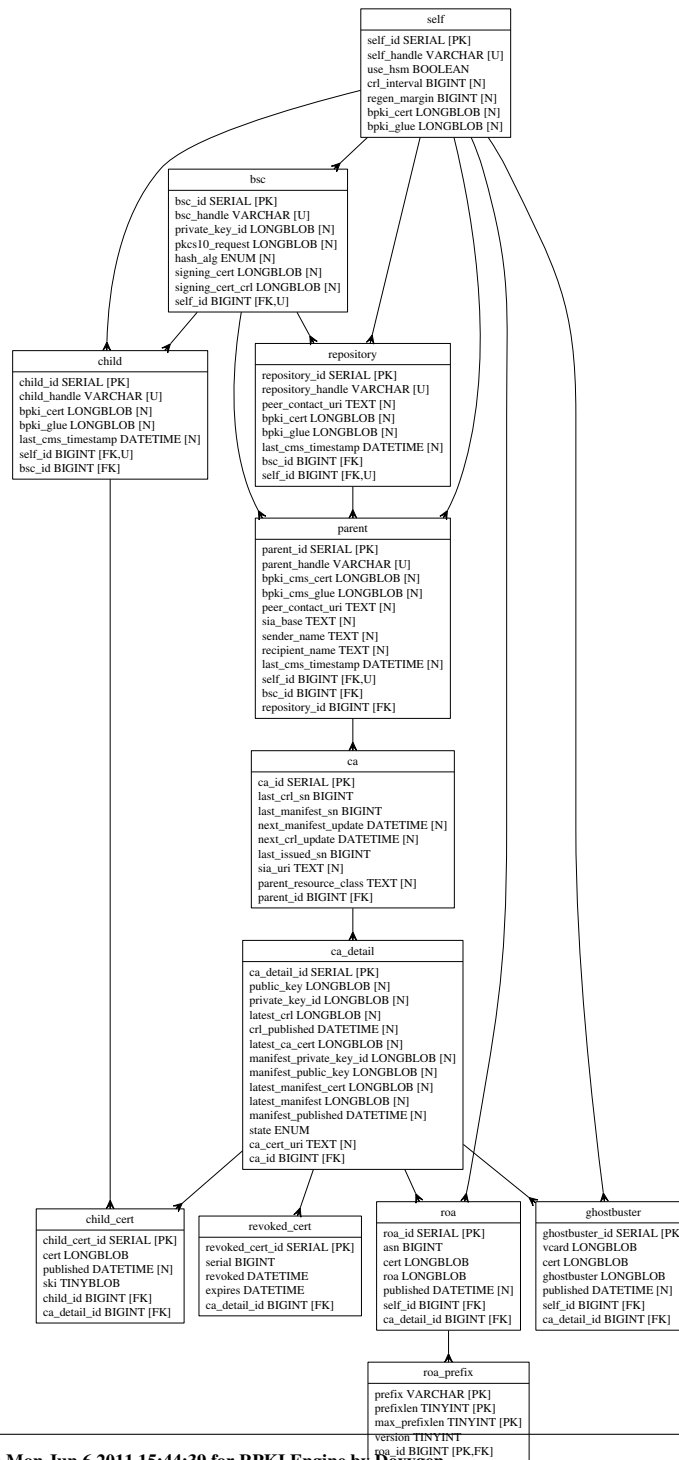
The previous paragraph only covers a "publish" action for a <certificate/> object. For "publish" actions on other objects, the publication server would need to trace permission back to the certificate issued by the parent; for "withdraw" actions, the publication server would have to perform the same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

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

9 SQL database schemas

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

9.1 rpkiid SQL schema



Generated on Mon Jun 6 2011 15:44:39 for RPKI Engine by Doxygen

Figure 1: Diagram of rpkiid.sql

```
-- $Id: rpkiid.sql 3745 2011-03-27 00:21:57Z sra $

-- Copyright (C) 2009--2011 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 (rpkiid.py).

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

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

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

```

        UNIQUE                                (self_handle)
    ) ENGINE=InnoDB;

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

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

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

```

```

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

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

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

CREATE TABLE child_cert (
    child_cert_id        SERIAL NOT NULL,
    cert                 LONGBLOB NOT NULL,
    published            DATETIME,
    ski                  TINYBLOB NOT NULL,

```



```

        child_id                BIGINT UNSIGNED NOT NULL,
        ca_detail_id            BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY              (child_cert_id),
        CONSTRAINT               child_cert_ca_detail_id
        FOREIGN KEY              (ca_detail_id) REFERENCES ca_detail (ca_detail_id) ON DELETE CASCADE
        CONSTRAINT               child_cert_child_id
        FOREIGN KEY              (child_id) REFERENCES child (child_id) ON DELETE CASCADE
    ) ENGINE=InnoDB;

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

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

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

CREATE TABLE ghostbuster (
    ghostbuster_id             SERIAL NOT NULL,
    vcard                       LONGBLOB NOT NULL,
    cert                       LONGBLOB NOT NULL,
    ghostbuster                 LONGBLOB NOT NULL,
    published                   DATETIME,
    self_id                     BIGINT UNSIGNED NOT NULL,
    ca_detail_id               BIGINT UNSIGNED NOT NULL,
    PRIMARY KEY                (ghostbuster_id),
    CONSTRAINT                 ghostbuster_self_id
    FOREIGN KEY                (self_id) REFERENCES self (self_id) ON DELETE CASCADE,

```

```

        CONSTRAINT
        FOREIGN KEY
    ) ENGINE=InnoDB;

ghostbuster_ca_detail_id
(ca_detail_id) REFERENCES ca_detail (ca_detail_id) ON DELETE CASCADE;

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

```

9.2 pubd SQL Schema

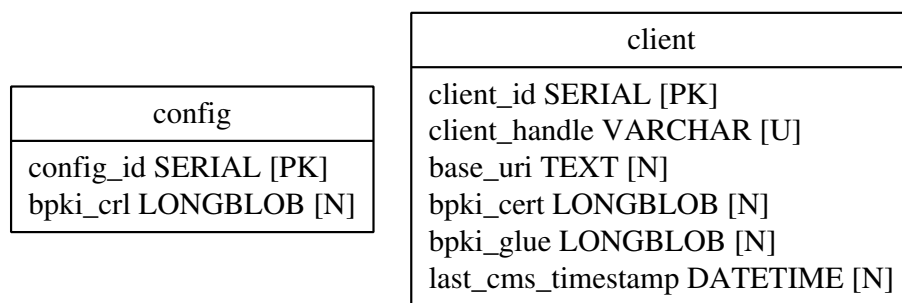


Figure 2: Diagram of pubd.sql

```

-- $Id: pubd.sql 3465 2010-10-07 00:59:39Z 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,
    bpkc_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,
    bpkc_cert          LONGBLOB,
    bpkc_glue          LONGBLOB,
    last_cms_timestamp DATETIME,
    PRIMARY KEY        (client_id),
    UNIQUE             (client_handle)
) ENGINE=InnoDB;

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

9.3 irdbd SQL Schema

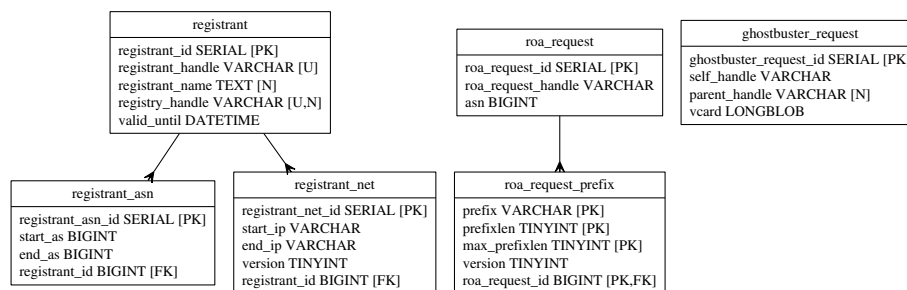


Figure 3: Diagram of irdbd.sql

```
-- $Id: irdbd.sql 3730 2011-03-21 12:42:43Z sra $
-- Copyright (C) 2009--2011 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;
DROP TABLE IF EXISTS ghostbuster_request;

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

CREATE TABLE registrant_asn (
    registrant_asn_id      SERIAL NOT NULL,
    start_as               BIGINT UNSIGNED NOT NULL,
    end_as                 BIGINT UNSIGNED NOT NULL,
    registrant_id          BIGINT UNSIGNED NOT NULL,
```

```

        PRIMARY KEY                (registrant_asn_id),
        CONSTRAINT                  registrant_asn_registrant_id
        FOREIGN KEY                  (registrant_id) REFERENCES registrant (registrant_id) ON DELETE CASCADE
    ) ENGINE=InnoDB;

CREATE TABLE registrant_net (
    registrant_net_id              SERIAL NOT NULL,
    start_ip                       VARCHAR(40) NOT NULL,
    end_ip                         VARCHAR(40) NOT NULL,
    version                        TINYINT UNSIGNED NOT NULL,
    registrant_id                  BIGINT UNSIGNED NOT NULL,
    PRIMARY KEY                    (registrant_net_id),
    CONSTRAINT                      registrant_net_registrant_id
    FOREIGN KEY                    (registrant_id) REFERENCES registrant (registrant_id) ON DELETE CASCADE
) ENGINE=InnoDB;

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

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

CREATE TABLE ghostbuster_request (
    ghostbuster_request_id        SERIAL NOT NULL,
    self_handle                   VARCHAR(40) NOT NULL,
    parent_handle                 VARCHAR(40),
    vcard                        LONGBLOB NOT NULL,
    PRIMARY KEY                   (ghostbuster_request_id)
) ENGINE=InnoDB;

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

```

10 BPKI model

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

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

relationships, hence the "B" (Business) in "BPKI".

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

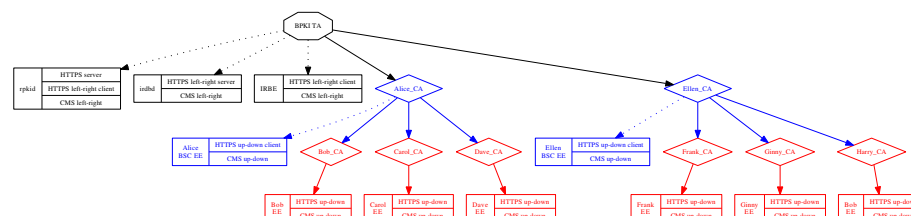
For the most part an ordinary user of this package need not worry about the details explained here, as the [myrpki tool](#) takes care of all of this. However, users who want to understand what's going on behind the scenes or who have needs too complex for the myrpki tool to handle might want to understand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

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

- Each engine should rely on a single BPKI trust anchor which is controlled by the back end entity that runs the engine; all other trust material should be cross-certified into the engine's BPKI tree.
- Private keys must never transit the network.
- Except for end entity certificates, the engine should only have access to the BPKI certificates; in particular, the private key for the BPKI trust anchor should not be accessible to the engine.
- The number of BPKI keys and certificates that the engine has to manage should be no larger than is necessary.

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

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



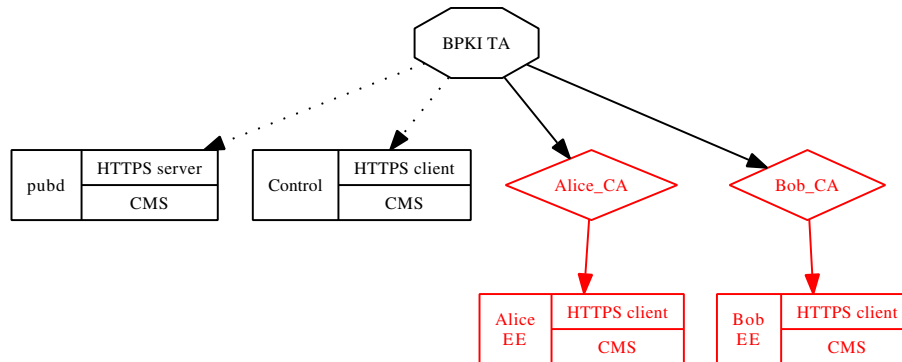
Black objects belong to the hosting entity, blue objects belong to the hosted entities, red objects are cross-certified objects from the hosted entities' peers. The arrows indicate certificate issuance: solid arrows are the ones that rpkid will care about during certificate validation, dotted arrows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

The certificate tree looks complicated, but the set of certificates needed to build any particular validation chain is obvious.

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 `rpkiid` instance, but is a bit simpler, as `pubd` does not provide hosting in the same sense that `rpkiid` 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 `rpkiid` and `pubd` instances, the two functions are conceptually separate. As far as `pubd` is concerned, it doesn't matter who operates the `rpkiid` instance: `pubd` just has clients, each of which has trust material that has been cross-certified into `pubd`'s BPKI. Similarly, `rpkiid` 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 `rpkiid` 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 `rpkiid` 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 `rpkiid` and `pubd` require

static configuration of the left-right and publication control certificates.

11 Todo List

Page Overview These explanations should be fleshed out properly.

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

12 Namespace Documentation

12.1 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 `cfg` = `rpki.config.parser(cfg_file, "irbe_cli")`
- `cfg_file` = `None`
- tuple `client_cert` = `rpki.x509.X509(Auto_file = cfg.get("rpkid-irbe-cert"))`
- tuple `client_key` = `rpki.x509.RSA(Auto_file = cfg.get("rpkid-irbe-key"))`
- `debug` = `verbose`)
- `pem_out` = `None`
- `proto` = `left_right_proto`,
- `q_msg` = `q_msg_left_right`
- list `q_msg_left_right` = `[]`
- list `q_msg_publication` = `[]`
- list `q_pdu` = `left_right_msg.pdus[argv[0]]`
- tuple `server_cert` = `rpki.x509.X509(Auto_file = cfg.get("rpkid-cert"))`
- tuple `server_ta` = `rpki.x509.X509(Auto_file = cfg.get("rpkid-bpki-ta"))`
- list `top_opts` = `["config=", "help", "pem_out=", "quiet", "verbose"]`
- tuple `url` = `cfg.get("rpkid-url")`
- tuple `usage_fill` = `UsageWrapper(subsequent_indent = " " * 4)`
- `verbose` = `True`

12.1.1 Detailed Description

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

\$Id: irbe_cli.py 3711 2011-03-03 14:01:23Z 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.

12.1.2 Function Documentation

12.1.2.1 `def irbe_cli.usage (code = 1)`

Definition at line 244 of file irbe_cli.py.

12.1.3 Variable Documentation

12.1.3.1 `tuple irbe_cli::argv = sys.argv[1:]`

Definition at line 264 of file irbe_cli.py.

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

Definition at line 288 of file irbe_cli.py.

12.1.3.3 `irbe_cli.cfg_file = None`

Definition at line 269 of file irbe_cli.py.

12.1.3.4 `tuple irbe_cli::client_cert = rpki.x509.X509(Auto_file =
cfg.get("rpkid-irbe-cert"))`

Definition at line 314 of file irbe_cli.py.

12.1.3.5 `tuple irbe_cli::client_key = rpki.x509.RSA(Auto_file =
cfg.get("rpkid-irbe-key"))`

Definition at line 313 of file irbe_cli.py.

12.1.3.6 `irbe_cli.debug = verbose))`

Definition at line 318 of file irbe_cli.py.

12.1.3.7 `irbe_cli.pem_out = None`

Definition at line 39 of file irbe_cli.py.

12.1.3.8 `irbe_cli.proto = left_right_proto,`

Definition at line 312 of file irbe_cli.py.

12.1.3.9 `irbe_cli.q_msg = q_msg_left_right`

Definition at line 296 of file irbe_cli.py.

12.1.3.10 `list irbe_cli.q_msg_left_right = []`

Definition at line 290 of file irbe_cli.py.

12.1.3.11 `list irbe_cli.q_msg_publication = []`

Definition at line 291 of file irbe_cli.py.

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

Definition at line 295 of file irbe_cli.py.

12.1.3.13 `tuple irbe_cli::server_cert = rpki.x509.X509(Auto_file =
cfg.get("rpki-cert"))`

Definition at line 316 of file irbe_cli.py.

12.1.3.14 `tuple irbe_cli::server_ta = rpki.x509.X509(Auto_file =
cfg.get("rpki-bpki-ta"))`

Definition at line 315 of file irbe_cli.py.

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

Definition at line 242 of file irbe_cli.py.

12.1.3.16 `tuple irbe_cli::url = cfg.get("rpki-url")`

Definition at line 317 of file irbe_cli.py.

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

Definition at line 52 of file irbe_cli.py.

12.1.3.18 irbe_cli.verbose = True

Definition at line 270 of file irbe_cli.py.

12.2 Package irbdb

12.2.1 Detailed Description

```
$Id: irbdb.py 3569 2010-12-14 20:35:28Z 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.

12.3 Package pubd

12.3.1 Detailed Description

```
$Id: pubd.py 3569 2010-12-14 20:35:28Z 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.

12.4 Package rootd

12.4.1 Detailed Description

\$Id: rootd.py 3569 2010-12-14 20:35:28Z 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.

12.5 Package rpki

Packages

- package [__doc__](#)
- package [adns](#)
- package [async](#)
- package [cli](#)
- package [config](#)
- package [exceptions](#)
- package [http](#)
- package [ipaddrs](#)
- package [irdbd](#)
- package [left_right](#)
- package [log](#)
- package [manifest](#)
- package [myrpki](#)
- package [oids](#)
- package [pubd](#)
- package [publication](#)
- package [relaxng](#)
- package [resource_set](#)
- package [roa](#)
- package [rootd](#)
- package [rpkid](#)
- package [sql](#)

- package [sundial](#)
- package [up_down](#)
- package [x509](#)
- package [xml_utils](#)

12.6 Package rpki.__doc__

12.7 Package rpki.adns

Classes

- class [dispatcher](#)
- class [getaddrinfo](#)
- class [query](#)
- class [test_getaddrinfo](#)
- class [test_query](#)

Variables

- list [nameservers](#) = []
Nameservers from resolver.nameservers converted to (af, address) pairs.
- tuple [resolver](#) = dns.resolver.Resolver()
Resolver object, shared by everything using this module.

12.7.1 Detailed Description

Basic asynchronous DNS code, using `asyncore` and Bob Halley's excellent `dnspython` package.

```
$Id: adns.py 3465 2010-10-07 00:59:39Z 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.

Portions copyright (C) 2003--2007, 2009, 2010 Nominum, Inc.

Permission to use, copy, modify, and distribute this software and its documentation 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 NOMINUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NOMINUM 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.

12.7.2 Variable Documentation

12.7.2.1 `rpki::adns::nameservers = []`

Nameservers from `resolver.nameservers` converted to (af, address) pairs.

The latter turns out to be a more useful form for us to use internally, because it simplifies the checks we need to make upon packet reception.

Definition at line 62 of file `adns.py`.

12.7.2.2 `rpki::adns::resolver = dns.resolver.Resolver()`

Resolver object, shared by everything using this module.

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

12.8 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`

12.8.1 Detailed Description

Utilities for event-driven programming.

\$Id: async.py 3793 2011-04-27 04:34:52Z 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.

12.8.2 Function Documentation

12.8.2.1 `def rpki.async._raiseExitNow (signum, frame) [private]`

Signal handler for `event_loop()`.

Definition at line 274 of file `async.py`.

12.8.2.2 `def rpki.async.defer (thunk)`

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

Definition at line 255 of file async.py.

12.8.2.3 `def rpki.async.event_loop (catch_signals =
 (signal.SIGINT, signal.SIGTERM)`

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

Definition at line 280 of file async.py.

12.8.2.4 `def rpki.async.exit_event_loop ()`

Force exit from `event_loop()`.

Definition at line 371 of file async.py.

12.8.2.5 `def rpki.async.run_deferred ()`

Run deferred actions.

Definition at line 261 of file async.py.

12.8.3 Variable Documentation

12.8.3.1 `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 253 of file async.py.

12.8.3.2 `rpki::async.ExitNow = asyncore.ExitNow`

Definition at line 24 of file async.py.

12.9 Package rpki.cli

Classes

- class `Cmd`

Functions

- def `yes_or_no`

Variables

- dictionary `_yes_or_no_prompts`
- `have_readline` = True

12.9.1 Detailed Description

Utilities for writing command line tools.

\$Id: cli.py 3255 2010-05-20 03:03:48Z 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.

12.9.2 Function Documentation

12.9.2.1 `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.

12.9.3 Variable Documentation

12.9.3.1 dictionary rpki::cli._yes_or_no_prompts

Initial value:

```
1 {
2   True   : ' ("yes" or "no" ["yes"]) ',
3   False  : ' ("yes" or "no" ["no"]) ',
4   None   : ' ("yes" or "no") ' }
```

Definition at line 172 of file cli.py.

12.9.3.2 rpki::cli.have_readline = True

Definition at line 25 of file cli.py.

12.10 Package rpki.config

Classes

- class [parser](#)

Variables

- [default_dirname](#) = None
Default name of directory to check for global config file, or None if no global config file.
- string [default_envname](#) = "RPKI_CONF"
Name of environment variable containing config file name.
- string [default_filename](#) = "rpki.conf"
Default name of config file if caller doesn't specify one explicitly.

12.10.1 Detailed Description

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

\$Id: config.py 3620 2011-01-20 19:59:13Z 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.

12.10.2 Variable Documentation

12.10.2.1 rpki::config::default_dirname = None

Default name of directory to check for global config file, or None if no global config file.

Autoconf-generated code may set this to a non-None value during script startup.

Definition at line 48 of file config.py.

12.10.2.2 rpki::config::default_envname = "RPKI_CONF"

Name of environment variable containing config file name.

Definition at line 53 of file config.py.

12.10.2.3 rpki::config::default_filename = "rpki.conf"

Default name of config file if caller doesn't specify one explicitly.

Definition at line 41 of file config.py.

12.11 Package rpki.exceptions

Classes

- class [BadClassNameSyntax](#)
- class [BadClientURL](#)
- class [BadContactURL](#)
- class [BadExtension](#)
- class [BadIPResource](#)
- class [BadIRDBReply](#)
- class [BadIssueResponse](#)
- class [BadPKCS10](#)
- class [BadPublicationReply](#)
- class [BadQuery](#)
- class [BadROAPrefix](#)
- 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 [CommandParseFailure](#)
- class [DBConsistencyError](#)
- class [DERObjectConversionError](#)
- class [DuplicateObject](#)
- class [EmptyPEM](#)
- class [EmptyROAPrefixList](#)
- class [ForbiddenURI](#)
- class [HandleTranslationError](#)
- class [HTTPBadVersion](#)
- class [HTTPClientAborted](#)
- class [HTTPRequestFailed](#)
- class [HTTPTimeout](#)

- class [HTTPUnexpectedState](#)
- class [MissingCMSCRL](#)
- class [MissingCMSEECert](#)
- class [MultipleTLSEECert](#)
- class [MustBePrefix](#)
- class [NoActiveCA](#)
- class [NoCoveringCertForROA](#)
- class [NoObjectAtURI](#)
- class [NotACertificateChain](#)
- class [NotFound](#)
- class [NotImplementedYet](#)
- class [NotInDatabase](#)
- class [ReceivedTLSCACert](#)
- class [RPKI_Exception](#)
- class [ServerShuttingDown](#)
- class [SKIMismatch](#)
- class [SubprocessError](#)
- class [TLSValidationError](#)
- class [UnexpectedCMSCerts](#)
- class [UnexpectedCMSCRLs](#)
- class [UnparsableCMSDER](#)
- class [UpstreamError](#)
- class [WrongEContentType](#)

12.11.1 Detailed Description

Exception definitions for RPKI modules.

```
$Id: exceptions.py 3465 2010-10-07 00:59:39Z 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.

12.12 Package rpki.http

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 [addr_to_string](#)
- def [client](#)
- def [localhost_addrinfo](#)
- def [log_method](#)
- def [server](#)
- def [supported_address_families](#)

Variables

- dictionary [client_queues](#) = { }
Map of (host, port) tuples to [http_queue](#) objects.
- [debug_http](#) = False
Verbose chatter about HTTP streams.
- 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.
- int `default_tcp_port` = 80
Default port for clients and servers that don't specify one.
- `enable_ipv6_clients` = False
Whether to consider IPv6 addresses when making connections.
- `enable_ipv6_servers` = True
Whether to enable IPv6 listeners.
- `have_ipv6` = False
Whether the current machine claims to support IPv6.
- string `rpki_content_type` = "application/x-rpki"
HTTP content type used for all RPKI messages.
- `use_adns` = False
Whether to use `rpki.adns` code.
- `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.

12.12.1 Detailed Description

HTTP utilities, both client and server.

\$Id: http.py 3793 2011-04-27 04:34:52Z sra \$

Copyright (C) 2009-2011 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.

12.12.2 Function Documentation

12.12.2.1 `def rpki.http.addr_to_string (addr)`

Convert socket addr tuple to printable string. Assumes 2-element tuple is IPv4, 4-element tuple is IPv6, throws TypeError for anything else.

Definition at line 285 of file http.py.

12.12.2.2 `def rpki.http.client (msg, url, callback, errback)`

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

Definition at line 930 of file http.py.

12.12.2.3 `def rpki.http.localhost_addrinfo ()`

Return pseudo-getaddrinfo results for localhost.

Definition at line 116 of file http.py.

12.12.2.4 def rpki.http.log_method (self, msg, logger = rpki.log.debug)

Logging method used in several different classes.

Definition at line 277 of file http.py.

12.12.2.5 def rpki.http.server (handlers, port, host = "")

Run an HTTP server and wait (forever) for connections.

Definition at line 973 of file http.py.

12.12.2.6 def rpki.http.supported_address_families (enable_ipv6)

IP address families on which servers should listen, and to consider when selecting addresses for client connections.

Definition at line 106 of file http.py.

12.12.3 Variable Documentation**12.12.3.1 rpki::http::client_queues = {}**

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

Definition at line 928 of file http.py.

12.12.3.2 rpki::http::debug_http = False

Verbose chatter about HTTP streams.

Definition at line 45 of file http.py.

12.12.3.3 rpki::http::default_client_timeout = rpki.sundial.timedelta(minutes = 15)

Default HTTP client connection timeout.

Definition at line 57 of file http.py.

12.12.3.4 rpki::http::default_http_version = (1, 0)

Preferred HTTP version.

Definition at line 68 of file http.py.

12.12.3.5 rpki::http::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 64 of file http.py.

12.12.3.6 rpki::http::default_tcp_port = 80

Default port for clients and servers that don't specify one.

Definition at line 72 of file http.py.

12.12.3.7 rpki::http::enable_ipv6_clients = False

Whether to consider IPv6 addresses when making connections.

Disabled by default, as IPv6 connectivity is still a bad joke in far too much of the world.

Definition at line 83 of file http.py.

12.12.3.8 rpki::http::enable_ipv6_servers = True

Whether to enable IPv6 listeners.

Enabled by default, as it should be harmless. Has no effect if kernel doesn't support IPv6.

Definition at line 77 of file http.py.

12.12.3.9 rpki::http::have_ipv6 = False

Whether the current machine claims to support IPv6.

Note that just because the kernel supports it doesn't mean that the machine has usable IPv6 connectivity. I don't know of a simple portable way to probe for connectivity at runtime (the old test of "can you ping SRI-NIC.ARPA?" seems a bit dated...). Don't set this, it's set automatically by probing using the socket() system call at runtime.

Definition at line 102 of file http.py.

12.12.3.10 rpki::http::rpki_content_type = "application/x-rpki"

HTTP content type used for all RPKI messages.

Definition at line 41 of file http.py.

12.12.3.11 rpki::http::use_adns = False

Whether to use [rpki.adns](#) code.

This is still experimental, so it's not (yet) enabled by default.

Definition at line 88 of file http.py.

12.12.3.12 rpki::http::want_persistent_client = False

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

Definition at line 49 of file http.py.

12.12.3.13 rpki::http::want_persistent_server = False

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

Definition at line 53 of file http.py.

12.13 Package rpki.ipaddrs

Classes

- class `v4addr`
- class `v6addr`

Functions

- def `parse`

12.13.1 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 3551 2010-11-14 23:28:45Z 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.

12.13.2 Function Documentation

12.13.2.1 def rpki.ipaddrs.parse (s)

Parse a string as either an IPv4 or IPv6 address, and return object of appropriate class.

Definition at line 122 of file ipaddrs.py.

12.14 Package rpki.irdbd

Classes

- class [main](#)

12.14.1 Detailed Description

IR database daemon.

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

\$Id: irdbd.py 3793 2011-04-27 04:34:52Z sra \$

Copyright (C) 2009--2011 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.

12.15 Package rpki.left_right

Classes

- class [bsc_elt](#)
- class [child_elt](#)
- class [cms_msg](#)
- class [data_elt](#)
- class [left_right_namespace](#)
- class [list_ghostbuster_requests_elt](#)
- 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

12.15.1 Detailed Description

RPKI "left-right" protocol.

\$Id: left_right.py 3793 2011-04-27 04:34:52Z sra \$

Copyright (C) 2009--2011 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.

12.15.2 Variable Documentation

12.15.2.1 `rpki::left_right.enforce_strict_up_down_xml_sender = False`

Definition at line 40 of file `left_right.py`.

12.16 Package rpki.log

Classes

- class `logger`

Functions

- def `init`
- def `log_repr`
- 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`
- `show_python_ids` = `False`

Whether `__repr__()` methods should show Python id numbers.

- string `tag` = `""`
- `use_syslog` = `True`

Whether to use syslog.

- tuple `warn` = `logger(syslog.LOG_WARNING)`

12.16.1 Detailed Description

Logging facilities for RPKI libraries.

\$Id: log.py 3793 2011-04-27 04:34:52Z 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.

12.16.2 Function Documentation

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

Initialize logging system.

Definition at line 56 of file log.py.

12.16.2.2 `def rpki.log.log_repr (obj, tokens)`

Constructor for `__repr__()` strings, handles suppression of Python IDs as needed.

Definition at line 118 of file log.py.

12.16.2.3 `def rpki.log.set_trace (enable)`

Enable or disable call tracing.

Definition at line 68 of file log.py.

12.16.2.4 `def rpki.log.trace ()`

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

Definition at line 96 of file log.py.

12.16.2.5 `def rpki.log.traceback ()`

Consolidated backtrace facility with a bit of extra info.

Definition at line 105 of file log.py.

12.16.3 Variable Documentation

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

Definition at line 94 of file log.py.

12.16.3.2 rpki::log::enable_trace = False

Whether call tracing is enabled.

Definition at line 41 of file log.py.

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

Definition at line 90 of file log.py.

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

Definition at line 93 of file log.py.

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

Definition at line 92 of file log.py.

12.16.3.6 int rpki::log.pid = 0

Definition at line 54 of file log.py.

12.16.3.7 rpki::log::show_python_ids = False

Whether `__repr__()` methods should show Python id numbers.

Definition at line 51 of file log.py.

12.16.3.8 string rpki::log.tag = ""

Definition at line 53 of file log.py.

12.16.3.9 rpki::log::use_syslog = True

Whether to use syslog.

Definition at line 46 of file log.py.

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

Definition at line 91 of file log.py.

12.17 Package rpki.manifest

Classes

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

12.17.1 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 3598 2011-01-04 05:12:16Z 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.

12.18 Package rpki.myrpki

Classes

- class [CA](#)
- class [child](#)
- class [children](#)
- class [comma_set](#)
- class [csv_reader](#)
- class [csv_writer](#)
- class [EntityDB](#)
- class [IRDB](#)
- class [main](#)
- class [parent](#)
- class [parents](#)
- class [repositories](#)
- class [repository](#)
- class [roa_request](#)
- class [roa_requests](#)

Functions

- def [b64_equal](#)
- def [etree_post_read](#)
- def [etree_pre_write](#)
- def [etree_read](#)
- def [etree_validate](#)
- def [etree_write](#)
- def [PEMBase64](#)
- def [PEMElement](#)

Variables

- [allow_incomplete](#) = False
- string [namespace](#) = "http://www.hactrn.net/uris/rpki/myrpki/"
- string [namespaceQName](#) = "{ "
- string [version](#) = "2"
- [whine](#) = True

12.18.1 Detailed Description

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

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

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

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

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

\$Id: myrpki.py 3793 2011-04-27 04:34:52Z sra \$

Copyright (C) 2009--2011 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.

12.18.2 Function Documentation

12.18.2.1 `def rpki.myrpki.b64_equal (thing1, thing2)`

Compare two Base64-encoded values for equality.

Definition at line 883 of file myrpki.py.

12.18.2.2 `def rpki.myrpki.etree_post_read (e, validate = True)`

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

Definition at line 869 of file myrpki.py.

12.18.2.3 `def rpki.myrpki.etree_pre_write (e, validate = True)`

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

Definition at line 844 of file myrpki.py.

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

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

Definition at line 859 of file myrpki.py.

12.18.2.5 `def rpki.myrpki.etree_validate (e)`

Definition at line 808 of file myrpki.py.

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

Write out an etree to a file, safely.

I still miss SYSCAL(RENWOW) .

Definition at line 825 of file myrpki.py.

12.18.2.7 `def rpki.myrpki.PEMBase64 (filename)`

Extract Base64 encoded data from a PEM file.

Definition at line 548 of file myrpki.py.

12.18.2.8 `def rpki.myrpki.PEMElement (e, tag, filename, kwargs)`

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

Definition at line 561 of file myrpki.py.

12.18.3 Variable Documentation

12.18.3.1 `rpki::myrpki.allow_incomplete = False`

Definition at line 80 of file myrpki.py.

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

Definition at line 74 of file myrpki.py.

12.18.3.3 string rpki::myrpki.namespaceQName = "{}"

Definition at line 76 of file myrpki.py.

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

Definition at line 75 of file myrpki.py.

12.18.3.5 rpki::myrpki.whine = True

Definition at line 84 of file myrpki.py.

12.19 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.

12.19.1 Detailed Description

OID database.

```
$Id: oids.py 3725 2011-03-18 03:51:12Z sra $
```

```
Copyright (C) 2009--2011 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.

12.19.2 Variable Documentation

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

Mapping table of string names to OIDs.

Definition at line 74 of file oids.py.

12.19.2.2 `rpki::oids::oid2name`

Mapping table of OIDs to conventional string names.

Definition at line 39 of file oids.py.

12.20 Package rpki.pubd

Classes

- class `main`

12.20.1 Detailed Description

RPKI publication engine.

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

\$Id: pubd.py 3793 2011-04-27 04:34:52Z 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.

12.21 Package rpki.publication

Classes

- class [certificate_elt](#)
- class [client_elt](#)
- class [cms_msg](#)
- class [config_elt](#)
- class [control_elt](#)
- class [crl_elt](#)
- class [ghostbuster_elt](#)
- class [manifest_elt](#)
- class [msg](#)
- class [publication_namespace](#)
- class [publication_object_elt](#)
- class [report_error_elt](#)
- class [roa_elt](#)
- class [sax_handler](#)

12.21.1 Detailed Description

RPKI "publication" protocol.

\$Id: publication.py 3793 2011-04-27 04:34:52Z sra \$

Copyright (C) 2009--2011 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.

12.22 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.

12.22.1 Variable Documentation

12.22.1.1 rpki::relaxng::left_right

Parsed RelaxNG [left_right](#) schema.

Definition at line 7 of file relaxng.py.

12.22.1.2 rpki::relaxng::publication

Parsed RelaxNG publication schema.

Definition at line 1265 of file relaxng.py.

12.22.1.3 rpki::relaxng::up_down

Parsed RelaxNG [up_down](#) schema.

Definition at line 1011 of file relaxng.py.

12.23 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`
- def `test3`
- def `testprefix`

Variables

- string `inherit_token` = "<inherit>"
Token used to indicate inheritance in read and print syntax.
- tuple `re_address_range` = `re.compile("^([0-9]:a-fA-F+)-([0-9]:a-fA-F+)$")`
- tuple `re_asn_range` = `re.compile("^([0-9]+)-([0-9]+)$")`
- tuple `re_prefix` = `re.compile("^([0-9]:a-fA-F+)/([0-9]+)$")`
- tuple `re_prefix_with_maxlen` = `re.compile("^([0-9]:a-fA-F+)/([0-9]+)-([0-9]+)$")`

12.23.1 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 3688 2011-02-24 00:00:05Z melkins \$

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.

12.23.2 Function Documentation

12.23.2.1 `def rpki.resource_set.bs2long(bs, addrlen, fill) [private]`

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

Definition at line 632 of file resource_set.py.

12.23.2.2 `def rpki.resource_set.long2bs(number, addrlen, prefixlen = None, strip = None) [private]`

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

Definition at line 644 of file resource_set.py.

12.23.2.3 `def rpki.resource_set.rsplitt(rset, that) [private]`

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

Definition at line 270 of file resource_set.py.

12.23.2.4 def rpki.resource_set.test1 (t, s1, s2)

Definition at line 1039 of file resource_set.py.

12.23.2.5 def rpki.resource_set.test2 (t, s1, s2)

Definition at line 1072 of file resource_set.py.

12.23.2.6 def rpki.resource_set.test3 (t, s1, s2)

Definition at line 1085 of file resource_set.py.

12.23.2.7 def rpki.resource_set.testprefix (v)

Definition at line 1036 of file resource_set.py.

12.23.3 Variable Documentation**12.23.3.1 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.

**12.23.3.2 tuple rpki::resource_set.re_address_range =
re.compile("^([0-9:.-a-zA-F]+)-([0-9:.-a-zA-F]+)\$")**

Definition at line 51 of file resource_set.py.

**12.23.3.3 tuple rpki::resource_set.re_asn_range =
re.compile("^([0-9]+)-([0-9]+)\$")**

Definition at line 50 of file resource_set.py.

12.23.3.4 tuple rpki::resource_set.re_prefix = re.compile("^([0-9:~a-zA-Z]+)/([0-9]+)\$")

Definition at line 53 of file resource_set.py.

12.23.3.5 tuple rpki::resource_set.re_prefix_with_maxlen = re.compile("^([0-9:~a-zA-Z]+)/([0-9]+)-([0-9]+)\$")

Definition at line 52 of file resource_set.py.

12.24 Package rpki.roa

Classes

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

12.24.1 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 3598 2011-01-04 05:12:16Z 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
```

12.25 Package rpki.rootd

Classes

- class [cms_msg](#)
- class [issue_pdu](#)
- class [list_pdu](#)
- class [main](#)
- class [message_pdu](#)
- class [revoke_pdu](#)
- class [sax_handler](#)

Variables

- [rootd](#) = None

12.25.1 Detailed Description

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

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

\$Id: rootd.py 3793 2011-04-27 04:34:52Z 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.

12.25.2 Variable Documentation

12.25.2.1 rpki::rootd.rootd = None

Definition at line 44 of file rpki/rootd.py.

12.26 Package rpki.rpkid

Classes

- class [ca_detail_obj](#)
- class [ca_obj](#)
- class [child_cert_obj](#)
- class [ghostbuster_obj](#)
- class [main](#)
- class [publication_queue](#)
- class [revoked_cert_obj](#)
- class [roa_obj](#)

12.26.1 Detailed Description

RPKI engine daemon.

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

\$Id: rpkid.py 3793 2011-04-27 04:34:52Z 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.

12.27 Package rpki.sql**Classes**

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

12.27.1 Detailed Description

SQL interface code.

\$Id: sql.py 3551 2010-11-14 23:28:45Z 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.

12.28 Package rpki.sundial

Classes

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

Functions

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

12.28.1 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 3783 2011-04-21 22:01:02Z sra $

Copyright (C) 2009--2011 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.

```

12.28.2 Function Documentation

12.28.2.1 `def rpki.sundial._cast(x) [private]`

Cast result of arithmetic operations back into correct subtype.

Definition at line 290 of file sundial.py.

12.28.2.2 `def rpki.sundial.now()`

Get current timestamp.

Definition at line 50 of file sundial.py.

12.28.2.3 def rpki.sundial.test (t)

Definition at line 302 of file sundial.py.

12.29 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/"

12.29.1 Detailed Description

RPKI "up-down" protocol.

```
$Id: up_down.py 3746 2011-03-27 01:24:39Z sra $
```

```
Copyright (C) 2009--2011 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.

12.29.2 Variable Documentation

12.29.2.1 dictionary `rpki::up_down.nsmmap = { None : xmlns }`

Definition at line 41 of file `up_down.py`.

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

Definition at line 39 of file `up_down.py`.

12.30 Package rpki.x509

Classes

- class [CMS_object](#)
- class [CRL](#)
- class [DeadDrop](#)
- class [DER_CMS_object](#)
- class [DER_object](#)
- class [Ghostbuster](#)

- 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 [base64_with_linebreaks](#)
- def [calculate_SKI](#)
- def [POWify_OID](#)

12.30.1 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 3793 2011-04-27 04:34:52Z sra \$

Copyright (C) 2009--2011 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.

12.30.2 Function Documentation

12.30.2.1 `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 109 of file x509.py.

12.30.2.2 `def rpki.x509.base64_with_linebreaks (der)`

Encode DER (really, anything) as Base64 text, with linebreaks to keep the result (sort of) readable.

Definition at line 51 of file x509.py.

12.30.2.3 `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 60 of file x509.py.

12.30.2.4 `def rpki.x509.POWify_OID (oid)`

Utility function to convert tuple form of an OID to the dotted-decimal string form that rpki.POW uses.

Definition at line 799 of file x509.py.

12.31 Package rpki.xml_utils

Classes

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

12.31.1 Detailed Description

XML utilities.

```
$Id: xml_utils.py 3725 2011-03-18 03:51:12Z sra $
```

Copyright (C) 2009-2011 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.

12.32 Package rpkid

12.32.1 Detailed Description

```
$Id: rpkid.py 3569 2010-12-14 20:35:28Z sra $
```

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

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

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

13 Class Documentation

13.1 `async_chat` Class Reference

Inheritance diagram for `async_chat`:

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

- [http.py \(3793\)](#)

13.2 `dispatcher` Class Reference

Inheritance diagram for `dispatcher`:

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

- [http.py \(3793\)](#)

13.3 `Cmd` Class Reference

Inheritance diagram for `Cmd`:

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

- [cli.py \(3255\)](#)

13.4 `dict` Class Reference

Inheritance diagram for `dict`:

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

- [myrpki.py \(3793\)](#)

13.5 Exception Class Reference

Inheritance diagram for Exception:

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

- [exceptions.py \(3465\)](#)

13.6 irbe_cli.bsc_elt Class Reference

Inheritance diagram for irbe_cli.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.

13.6.1 Detailed Description

Definition at line 154 of file irbe_cli.py.

13.6.2 Member Function Documentation

13.6.2.1 def irbe_cli.bsc_elt.client_query_signing_cert (self, arg)

--signing_cert option.

Definition at line 158 of file irbe_cli.py.

13.6.2.2 def irbe_cli.bsc_elt.client_query_signing_cert_crl (self, arg)

--signing_cert_crl option.

Definition at line 162 of file irbe_cli.py.

13.6.2.3 def irbe_cli.bsc_elt.client_reply_decode (self)

Reimplemented from [irbe_cli.reply_elt_mixin](#).

Definition at line 166 of file irbe_cli.py.

13.6.3 Member Data Documentation

13.6.3.1 tuple irbe_cli.bsc_elt.excludes = ("pkcs10_request",) [static]

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

Reimplemented from [irbe_cli.cmd_elt_mixin](#).

Definition at line 156 of file irbe_cli.py.

13.6.3.2 irbe_cli.bsc_elt.signing_cert

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

Definition at line 158 of file irbe_cli.py.

13.6.3.3 irbe_cli.bsc_elt.signing_cert_crl

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

Definition at line 162 of file irbe_cli.py.

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

- [irbe_cli.py \(3711\)](#)

13.7 `irbe_cli.certificate_elt` Class Reference

Inheritance diagram for `irbe_cli.certificate_elt`:

Collaboration diagram for `irbe_cli.certificate_elt`:

13.7.1 Detailed Description

Definition at line 215 of file `irbe_cli.py`.

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

- [irbe_cli.py \(3711\)](#)

13.8 `irbe_cli.child_elt` Class Reference

Inheritance diagram for `irbe_cli.child_elt`:

Collaboration diagram for `irbe_cli.child_elt`:

13.8.1 Detailed Description

Definition at line 176 of file `irbe_cli.py`.

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

- [irbe_cli.py \(3711\)](#)

13.9 `irbe_cli.client_elt` Class Reference

Inheritance diagram for `irbe_cli.client_elt`:

Collaboration diagram for `irbe_cli.client_elt`:

13.9.1 Detailed Description

Definition at line 212 of file `irbe_cli.py`.

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

- [irbe_cli.py \(3711\)](#)

13.10 irbe_cli.cmd_elt_mixin Class Reference

Inheritance diagram for irbe_cli.cmd_elt_mixin:

Collaboration diagram for irbe_cli.cmd_elt_mixin:

Public Member Functions

- def [client_getopt](#)
- def [client_query_bpki_cert](#)
- def [client_query_bpki_cms_cert](#)
- def [client_query_cms_glue](#)
- def [client_query_glue](#)
- def [usage](#)

Public Attributes

- [bpki_cert](#)
- [bpki_cms_cert](#)
- [bpki_cms_glue](#)
- [bpki_glue](#)

Static Public Attributes

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

13.10.1 Detailed Description

Protocol mix-in for command line client element PDUs.

Definition at line 70 of file irbe_cli.py.

13.10.2 Member Function Documentation

13.10.2.1 def irbe_cli.cmd_elt_mixin.client_getopt (self, argv)

Parse options for this class.

Definition at line 94 of file irbe_cli.py.

13.10.2.2 def irbe_cli.cmd_elt_mixin.client_query_bpki_cert (self, arg)

Special handler for --bpki_cert option.

Definition at line 111 of file irbe_cli.py.

13.10.2.3 def irbe_cli.cmd_elt_mixin.client_query_bpki_cms_cert (self, arg)

Special handler for --bpki_cms_cert option.

Definition at line 123 of file irbe_cli.py.

13.10.2.4 def irbe_cli.cmd_elt_mixin.client_query_cms_glue (self, arg)

Special handler for --bpki_cms_glue option.

Definition at line 129 of file irbe_cli.py.

13.10.2.5 def irbe_cli.cmd_elt_mixin.client_query_glue (self, arg)

Special handler for --bpki_glue option.

Definition at line 117 of file irbe_cli.py.

13.10.2.6 def irbe_cli.cmd_elt_mixin.usage (cls)

Generate usage message for this PDU.

Definition at line 83 of file irbe_cli.py.

13.10.3 Member Data Documentation**13.10.3.1 irbe_cli.cmd_elt_mixin.bpki_cert**

Definition at line 113 of file irbe_cli.py.

13.10.3.2 `irbe_cli.cmd_elt_mixin.bpki_cms_cert`

Definition at line 125 of file `irbe_cli.py`.

13.10.3.3 `irbe_cli.cmd_elt_mixin.bpki_cms_glue`

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

13.10.3.4 `irbe_cli.cmd_elt_mixin.bpki_glue`

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

13.10.3.5 `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 80 of file `irbe_cli.py`.

13.10.3.6 `irbe_cli.cmd_elt_mixin.is_cmd = True` `[static]`

Reimplemented from [irbe_cli.reply_elt_mixin](#).

Definition at line 75 of file `irbe_cli.py`.

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

- [irbe_cli.py \(3711\)](#)

13.11 `irbe_cli.cmd_msg_mixin` Class Reference

Inheritance diagram for `irbe_cli.cmd_msg_mixin`:

Collaboration diagram for `irbe_cli.cmd_msg_mixin`:

Public Member Functions

- def [usage](#)

13.11.1 Detailed Description

Protocol mix-in for command line client message PDUs.

Definition at line 135 of file `irbe_cli.py`.

13.11.2 Member Function Documentation

13.11.2.1 def `irbe_cli.cmd_msg_mixin.usage (cls)`

Generate usage message for this PDU.

Definition at line 141 of file `irbe_cli.py`.

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

- [irbe_cli.py \(3711\)](#)

13.12 irbe_cli.config_elt Class Reference

Inheritance diagram for `irbe_cli.config_elt`:

Collaboration diagram for `irbe_cli.config_elt`:

Public Member Functions

- def [client_query_bpki_crl](#)

Public Attributes

- [bpki_crl](#)

13.12.1 Detailed Description

Definition at line 204 of file `irbe_cli.py`.

13.12.2 Member Function Documentation

13.12.2.1 def irbe_cli.config_elt.client_query_bpki_crl (self, arg)

Special handler for --bpki_crl option.

Definition at line 206 of file irbe_cli.py.

13.12.3 Member Data Documentation

13.12.3.1 irbe_cli.config_elt.bpki_crl

Definition at line 208 of file irbe_cli.py.

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

- [irbe_cli.py \(3711\)](#)

13.13 irbe_cli.crl_elt Class Reference

Inheritance diagram for irbe_cli.crl_elt:

Collaboration diagram for irbe_cli.crl_elt:

13.13.1 Detailed Description

Definition at line 218 of file irbe_cli.py.

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

- [irbe_cli.py \(3711\)](#)

13.14 irbe_cli.left_right_cms_msg Class Reference

Inheritance diagram for irbe_cli.left_right_cms_msg:

Collaboration diagram for irbe_cli.left_right_cms_msg:

Static Public Attributes

- [saxify](#) = left_right_sax_handler.saxify

13.14.1 Detailed Description

Definition at line 199 of file irbe_cli.py.

13.14.2 Member Data Documentation

13.14.2.1 irbe_cli.left_right_msg.saxify = left_right_sax_handler.saxify [static]

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

Definition at line 200 of file irbe_cli.py.

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

- [irbe_cli.py \(3711\)](#)

13.15 irbe_cli.left_right_msg Class Reference

Inheritance diagram for irbe_cli.left_right_msg:

Collaboration diagram for irbe_cli.left_right_msg:

Static Public Attributes

- tuple [pdus](#)
Dispatch table of PDUs for this protocol.

13.15.1 Detailed Description

Definition at line 191 of file irbe_cli.py.

13.15.2 Member Data Documentation

13.15.2.1 tuple irbe_cli.left_right_msg.pdus [static]

Initial value:

```
dict((x.element_name, x)
      for x in (self_elt, bsc_elt, parent_elt, child_elt, repository_elt,
               list_published_objects_elt, list_received_resources_elt,
               report_error_elt))
```

Dispatch table of PDUs for this protocol.

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

Definition at line 192 of file irbe_cli.py.

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

- [irbe_cli.py \(3711\)](#)

13.16 irbe_cli.left_right_proto Class Reference

Inheritance diagram for irbe_cli.left_right_proto:

Collaboration diagram for irbe_cli.left_right_proto:

Static Public Attributes

- [cms_msg = left_right_cms_msg](#)
- [msg = left_right_msg](#)

13.16.1 Detailed Description

Definition at line 307 of file irbe_cli.py.

13.16.2 Member Data Documentation

13.16.2.1 irbe_cli.left_right_proto.cms_msg = left_right_cms_msg [static]

Definition at line 308 of file irbe_cli.py.

13.16.2.2 irbe_cli.left_right_proto.msg = left_right_msg [static]

Definition at line 309 of file irbe_cli.py.

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

- [irbe_cli.py \(3711\)](#)

13.17 `irbe_cli.left_right_sax_handler` Class Reference

Inheritance diagram for `irbe_cli.left_right_sax_handler`:

Collaboration diagram for `irbe_cli.left_right_sax_handler`:

Static Public Attributes

- `pdu = left_right_msg`

13.17.1 Detailed Description

Definition at line 196 of file `irbe_cli.py`.

13.17.2 Member Data Documentation

13.17.2.1 `irbe_cli.left_right_sax_handler.pdu = left_right_msg` [static]

Reimplemented from `rpki.left_right.sax_handler`.

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

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

- `irbe_cli.py` (3711)

13.18 `irbe_cli.list_published_objects_elt` Class Reference

Inheritance diagram for `irbe_cli.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.

13.18.1 Detailed Description

Definition at line 182 of file `irbe_cli.py`.

13.18.2 Member Data Documentation

13.18.2.1 `tuple irbe_cli.list_published_objects_elt.excludes = ("uri",)` `[static]`

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

Reimplemented from [irbe_cli.cmd_elt_mixin](#).

Definition at line 183 of file `irbe_cli.py`.

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

- [irbe_cli.py \(3711\)](#)

13.19 `irbe_cli.list_received_resources_elt` Class Reference

Inheritance diagram for `irbe_cli.list_received_resources_elt`:

Collaboration diagram for `irbe_cli.list_received_resources_elt`:

Static Public Attributes

- `tuple excludes = ("parent_handle", "notBefore", "notAfter", "uri", "sia_uri", "aia_uri", "asn", "ipv4", "ipv6")`

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

13.19.1 Detailed Description

Definition at line 185 of file `irbe_cli.py`.

13.19.2 Member Data Documentation

13.19.2.1 `tuple irbe_cli.list_received_resources_elt.excludes =` `("parent_handle", "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 186 of file `irbe_cli.py`.

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

- [irbe_cli.py \(3711\)](#)

13.20 `irbe_cli.manifest_elt` Class Reference

Inheritance diagram for `irbe_cli.manifest_elt`:

Collaboration diagram for `irbe_cli.manifest_elt`:

13.20.1 Detailed Description

Definition at line 221 of file `irbe_cli.py`.

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

- [irbe_cli.py \(3711\)](#)

13.21 `irbe_cli.parent_elt` Class Reference

Inheritance diagram for `irbe_cli.parent_elt`:

Collaboration diagram for `irbe_cli.parent_elt`:

13.21.1 Detailed Description

Definition at line 173 of file `irbe_cli.py`.

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

- [irbe_cli.py \(3711\)](#)

13.22 `irbe_cli.publication.cms_msg` Class Reference

Inheritance diagram for `irbe_cli.publicationcms_msg`:

Collaboration diagram for `irbe_cli.publicationcms_msg`:

Static Public Attributes

- `saxify` = `publication_sax_handler.saxify`

13.22.1 Detailed Description

Definition at line 237 of file `irbe_cli.py`.

13.22.2 Member Data Documentation

13.22.2.1 `irbe_cli.publication_msg.saxify = publication_sax_handler.saxify` [static]

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

Definition at line 238 of file `irbe_cli.py`.

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

- [irbe_cli.py \(3711\)](#)

13.23 `irbe_cli.publication_msg` Class Reference

Inheritance diagram for `irbe_cli.publication_msg`:

Collaboration diagram for `irbe_cli.publication_msg`:

Static Public Attributes

- tuple [pdus](#)
Dispatch table of PDUs for this protocol.

13.23.1 Detailed Description

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

13.23.2 Member Data Documentation

13.23.2.1 tuple `irbe_cli.publication_msg.pdus` [static]

Initial value:

```
dict((x.element_name, x)
      for x in (config_elt, client_elt, certificate_elt, crl_elt, manifes
                t_elt, roa_elt, report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented from [rpki.publication.msg](#).

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

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

- [irbe_cli.py \(3711\)](#)

13.24 `irbe_cli.publication_proto` Class Reference

Inheritance diagram for `irbe_cli.publication_proto`:

Collaboration diagram for `irbe_cli.publication_proto`:

Static Public Attributes

- `cms_msg` = `publication_cms_msg`
- `msg` = `publication_msg`

13.24.1 Detailed Description

Definition at line 324 of file `irbe_cli.py`.

13.24.2 Member Data Documentation

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

Definition at line 326 of file `irbe_cli.py`.

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

Definition at line 325 of file `irbe_cli.py`.

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

- [irbe_cli.py \(3711\)](#)

13.25 `irbe_cli.publication_sax_handler` Class Reference

Inheritance diagram for `irbe_cli.publication_sax_handler`:

Collaboration diagram for `irbe_cli.publication_sax_handler`:

Static Public Attributes

- `pdu = publication_msg`

13.25.1 Detailed Description

Definition at line 234 of file `irbe_cli.py`.

13.25.2 Member Data Documentation

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

Reimplemented from `rpki.publication.sax_handler`.

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

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

- `irbe_cli.py` (3711)

13.26 `irbe_cli.reply_elt_mixin` Class Reference

Inheritance diagram for `irbe_cli.reply_elt_mixin`:

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`

13.26.1 Detailed Description

Protocol mix-in for printout of reply PDUs.

Definition at line 54 of file `irbe_cli.py`.

13.26.2 Member Function Documentation

13.26.2.1 `def irbe_cli.reply_elt_mixin.client_reply_decode (self)`

Reimplemented in [irbe_cli.bsc_elt](#).

Definition at line 61 of file `irbe_cli.py`.

13.26.2.2 `def irbe_cli.reply_elt_mixin.client_reply_show (self)`

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

13.26.3 Member Data Documentation

13.26.3.1 `irbe_cli.reply_elt_mixin.is_cmd = False [static]`

Reimplemented in [irbe_cli.cmd_elt_mixin](#).

Definition at line 59 of file `irbe_cli.py`.

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

- [irbe_cli.py \(3711\)](#)

13.27 `irbe_cli.report_error_elt` Class Reference

Inheritance diagram for `irbe_cli.report_error_elt`:

Collaboration diagram for `irbe_cli.report_error_elt`:

13.27.1 Detailed Description

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

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

- [irbe_cli.py \(3711\)](#)

13.28 `irbe_cli.repository_elt` Class Reference

Inheritance diagram for `irbe_cli.repository_elt`:

Collaboration diagram for `irbe_cli.repository_elt`:

13.28.1 Detailed Description

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

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

- [irbe_cli.py \(3711\)](#)

13.29 `irbe_cli.roa_elt` Class Reference

Inheritance diagram for `irbe_cli.roa_elt`:

Collaboration diagram for `irbe_cli.roa_elt`:

13.29.1 Detailed Description

Definition at line 224 of file `irbe_cli.py`.

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

- [irbe_cli.py \(3711\)](#)

13.30 `irbe_cli.self_elt` Class Reference

Inheritance diagram for `irbe_cli.self_elt`:

Collaboration diagram for `irbe_cli.self_elt`:

13.30.1 Detailed Description

Definition at line 151 of file `irbe_cli.py`.

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

- [irbe_cli.py \(3711\)](#)

13.31 `irbe_cli.UsageWrapper` Class Reference

Inheritance diagram for `irbe_cli.UsageWrapper`:

Collaboration diagram for `irbe_cli.UsageWrapper`:

Public Member Functions

- `def __call__`

13.31.1 Detailed Description

Call interface around Python `textwrap.TextWrapper` class.

Definition at line 41 of file `irbe_cli.py`.

13.31.2 Member Function Documentation

13.31.2.1 `def irbe_cli.UsageWrapper.__call__(self, args)`

Format arguments, with `TextWrapper` indentation.

Definition at line 46 of file `irbe_cli.py`.

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

- [irbe_cli.py \(3711\)](#)

13.32 long Class Reference

Inheritance diagram for long:

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

- [ipaddrs.py \(3551\)](#)

13.33 object Class Reference

Inheritance diagram for object:

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

- [x509.py \(3793\)](#)

13.34 **datetime Class Reference**

Inheritance diagram for datetime:

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

- [sundial.py \(3783\)](#)

13.35 **timedelta Class Reference**

Inheritance diagram for timedelta:

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

- [sundial.py \(3783\)](#)

13.36 **rpki.adns.dispatcher Class Reference**

Inheritance diagram for rpki.adns.dispatcher:

Collaboration diagram for rpki.adns.dispatcher:

Public Member Functions

- def [__init__](#)
- def [handle_connect](#)
- def [handle_error](#)
- def [handle_read](#)
- def [writable](#)

Public Attributes

- [af](#)
- [bufsize](#)
- [cb](#)
- [eb](#)

13.36.1 Detailed Description

Basic UDP socket reader for use with `asyncore`.

Definition at line 77 of file `adns.py`.

13.36.2 Constructor & Destructor Documentation

13.36.2.1 `def rpki.adns.dispatcher.__init__(self, cb, eb, af, bufsize = 65535)`

Definition at line 82 of file adns.py.

13.36.3 Member Function Documentation

13.36.3.1 `def rpki.adns.dispatcher.handle_connect(self)`

Quietly ignore UDP "connection" events.

Definition at line 103 of file adns.py.

13.36.3.2 `def rpki.adns.dispatcher.handle_error(self)`

Pass errors to query class errback.

Definition at line 97 of file adns.py.

13.36.3.3 `def rpki.adns.dispatcher.handle_read(self)`

Receive a packet, hand it off to query class callback.

Definition at line 90 of file adns.py.

13.36.3.4 `def rpki.adns.dispatcher.writable(self)`

We don't need to hear about UDP socket becoming writable.

Definition at line 109 of file adns.py.

13.36.4 Member Data Documentation

13.36.4.1 rpki.adns.dispatcher.af

Definition at line 82 of file adns.py.

13.36.4.2 rpki.adns.dispatcher.bufsize

Definition at line 82 of file adns.py.

13.36.4.3 rpki.adns.dispatcher.cb

Definition at line 82 of file adns.py.

13.36.4.4 rpki.adns.dispatcher.eb

Definition at line 82 of file adns.py.

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

- [adns.py \(3465\)](#)

13.37 rpki.adns.getaddrinfo Class Reference

Inheritance diagram for rpki.adns.getaddrinfo:

Collaboration diagram for rpki.adns.getaddrinfo:

Public Member Functions

- def [__init__](#)
- def [done](#)
- def [lose](#)

Public Attributes

- [cb](#)
- [eb](#)
- [host](#)
- [queries](#)
- [result](#)

Static Public Attributes

- dictionary [typemap](#)

13.37.1 Detailed Description

Definition at line 294 of file adns.py.

13.37.2 Constructor & Destructor Documentation

13.37.2.1 `def rpki.adns.getaddrinfo.__init__(self, cb, eb, host, address_families = typemap.values())`

Definition at line 299 of file adns.py.

13.37.3 Member Function Documentation

13.37.3.1 `def rpki.adns.getaddrinfo.done(self, q, answer)`

Definition at line 308 of file adns.py.

13.37.3.2 `def rpki.adns.getaddrinfo.lose(self, q, e)`

Definition at line 316 of file adns.py.

13.37.4 Member Data Documentation

13.37.4.1 rpki.adns.getaddrinfo.cb

Definition at line 299 of file adns.py.

13.37.4.2 rpki.adns.getaddrinfo.eb

Definition at line 299 of file adns.py.

13.37.4.3 rpki.adns.getaddrinfo.host

Definition at line 299 of file adns.py.

13.37.4.4 rpki.adns.getaddrinfo.queries

Definition at line 299 of file adns.py.

13.37.4.5 rpki.adns.getaddrinfo.result

Definition at line 299 of file adns.py.

13.37.4.6 dictionary rpki.adns.getaddrinfo.typemap [static]

Initial value:

```
{ dns.rdatatype.A      : socket.AF_INET,
  dns.rdatatype.AAAA   : socket.AF_INET6 }
```

Definition at line 296 of file adns.py.

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

- [adns.py \(3465\)](#)

13.38 rpki.adns.query Class Reference

Inheritance diagram for rpki.adns.query:

Collaboration diagram for rpki.adns.query:

Public Member Functions

- def [__init__](#)
- def [cleanup](#)
- def [done1](#)
- def [done2](#)
- def [go](#)
- def [loop1](#)
- def [loop2](#)
- def [lose](#)
- def [socket_cb](#)
- def [socket_eb](#)
- def [socket_timeout](#)

Public Attributes

- [backoff](#)
- [cb](#)
- [eb](#)
- [iterator](#)
- [nameservers](#)
- [qclass](#)
- [qname](#)
- [qtype](#)
- [request](#)
- [response](#)
- [sockets](#)
- [start](#)
- [timer](#)

13.38.1 Detailed Description

Simplified (no search paths) asynchronous adaptation of `dns.resolver.Resolver.query()` (q.v.).

Definition at line 116 of file `adns.py`.

13.38.2 Constructor & Destructor Documentation

13.38.2.1 `def rpki.adns.query.__init__(self, cb, eb, qname, qtype = dns.rdatatype.A, qclass = dns.rdataclass.IN)`

Definition at line 122 of file adns.py.

13.38.3 Member Function Documentation

13.38.3.1 `def rpki.adns.query.cleanup(self)`

Shut down our timer and sockets.

Definition at line 258 of file adns.py.

13.38.3.2 `def rpki.adns.query.done1(self)`

Done with outer loop. If we got a useful answer, cache it, then pass it back to caller; if we got an error, pass the appropriate exception back to caller.

Definition at line 273 of file adns.py.

13.38.3.3 `def rpki.adns.query.done2(self)`

Done with inner loop. If we still haven't got an answer and haven't (yet?) eliminated all of our nameservers, wait a little while before starting the cycle again, unless we've hit the timeout threshold for the whole query.

Definition at line 239 of file adns.py.

13.38.3.4 `def rpki.adns.query.go(self)`

Start running the query. Check our cache before doing network query; if we find an answer there, just return it. Otherwise start the network query.

Definition at line 138 of file adns.py.

13.38.3.5 def rpki.adns.query.loop1 (*self*)

Outer loop. If we haven't got a response yet and still have nameservers to check, start inner loop. Otherwise, we're done.

Definition at line 162 of file adns.py.

13.38.3.6 def rpki.adns.query.loop2 (*self*, *iterator*, *nameserver*)

Inner loop. Send query to next nameserver in our list, unless we've hit the overall timeout for this query.

Definition at line 173 of file adns.py.

13.38.3.7 def rpki.adns.query.lose (*self*, *e*)

Something bad happened. Clean up, then pass error back to caller.

Definition at line 266 of file adns.py.

13.38.3.8 def rpki.adns.query.socket_cb (*self*, *af*, *from_host*, *from_port*, *wire*)

Received a packet that might be a DNS message. If it doesn't look like it came from one of our nameservers, just drop it and leave the timer running. Otherwise, try parsing it: if it's an answer, we're done, otherwise handle error appropriately and move on to next nameserver.

Definition at line 213 of file adns.py.

13.38.3.9 def rpki.adns.query.socket_eb (*self*, *e*)

UDP socket signaled error. If it really is some kind of socket error, handle as if we've timed out on this nameserver; otherwise, pass error back to caller.

Definition at line 200 of file adns.py.

13.38.3.10 def rpki.adns.query.socket_timeout (*self*)

No answer from nameserver, move on to next one (inner loop).

Definition at line 193 of file adns.py.

13.38.4 Member Data Documentation

13.38.4.1 rpki.adns.query.backoff

Definition at line 142 of file adns.py.

13.38.4.2 rpki.adns.query.cb

Definition at line 122 of file adns.py.

13.38.4.3 rpki.adns.query.eb

Definition at line 122 of file adns.py.

13.38.4.4 rpki.adns.query.iterator

Definition at line 165 of file adns.py.

13.38.4.5 rpki.adns.query.nameservers

Definition at line 142 of file adns.py.

13.38.4.6 rpki.adns.query.qclass

Definition at line 122 of file adns.py.

13.38.4.7 rpki.adns.query.qname

Definition at line 122 of file adns.py.

13.38.4.8 rpki.adns.query.qtype

Definition at line 122 of file adns.py.

13.38.4.9 rpki.adns.query.request

Definition at line 142 of file adns.py.

13.38.4.10 rpki.adns.query.response

Definition at line 142 of file adns.py.

13.38.4.11 rpki.adns.query.sockets

Definition at line 142 of file adns.py.

13.38.4.12 rpki.adns.query.start

Definition at line 122 of file adns.py.

13.38.4.13 rpki.adns.query.timer

Definition at line 142 of file adns.py.

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

- [adns.py \(3465\)](#)

13.39 rpki.adns.test_getaddrinfo Class Reference

Inheritance diagram for rpki.adns.test_getaddrinfo:

Collaboration diagram for rpki.adns.test_getaddrinfo:

Public Member Functions

- def [__init__](#)
- def [done](#)
- def [lose](#)

Public Attributes

- [qname](#)

13.39.1 Detailed Description

Definition at line 329 of file adns.py.

13.39.2 Constructor & Destructor Documentation

13.39.2.1 def rpki.adns.test_getaddrinfo.__init__(*self*, *qname*)

Definition at line 331 of file adns.py.

13.39.3 Member Function Documentation

13.39.3.1 def rpki.adns.test_getaddrinfo.done (*self*, *result*)

Definition at line 335 of file adns.py.

13.39.3.2 def rpki.adns.test_getaddrinfo.lose (self, e)

Definition at line 340 of file adns.py.

13.39.4 Member Data Documentation

13.39.4.1 rpki.adns.test_getaddrinfo.qname

Definition at line 331 of file adns.py.

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

- [adns.py \(3465\)](#)

13.40 rpki.adns.test_query Class Reference

Inheritance diagram for rpki.adns.test_query:

Collaboration diagram for rpki.adns.test_query:

Public Member Functions

- def [__init__](#)
- def [done](#)
- def [lose](#)

Public Attributes

- [qclass](#)
- [qname](#)
- [qtype](#)

13.40.1 Detailed Description

Definition at line 343 of file adns.py.

13.40.2 Constructor & Destructor Documentation

13.40.2.1 `def rpki.adns.test_query.__init__(self, qname, qtype = dns.rdatatype.A, qclass = dns.rdataclass.IN)`

Definition at line 345 of file adns.py.

13.40.3 Member Function Documentation

13.40.3.1 `def rpki.adns.test_query.done(self, q, result)`

Definition at line 351 of file adns.py.

13.40.3.2 `def rpki.adns.test_query.lose(self, q, e)`

Definition at line 358 of file adns.py.

13.40.4 Member Data Documentation

13.40.4.1 `rpki.adns.test_query.qclass`

Definition at line 345 of file adns.py.

13.40.4.2 `rpki.adns.test_query.qname`

Definition at line 345 of file adns.py.

13.40.4.3 `rpki.adns.test_query.qtype`

Definition at line 345 of file adns.py.

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

- [adns.py \(3465\)](#)

13.41 rpki.async.gc_summary Class Reference

Inheritance diagram for rpki.async.gc_summary:

Collaboration diagram for rpki.async.gc_summary:

Public Member Functions

- def [__init__](#)
- def [handler](#)

Public Attributes

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

13.41.1 Detailed Description

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

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

13.41.2 Constructor & Destructor Documentation

13.41.2.1 def rpki.async.gc_summary.__init__(self, interval, threshold = 0)

Definition at line 382 of file `async.py`.

13.41.3 Member Function Documentation

13.41.3.1 def rpki.async.gc_summary.handler(self)

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

Definition at line 390 of file `async.py`.

13.41.4 Member Data Documentation

13.41.4.1 rpki.async.gc_summary.interval

Definition at line 382 of file async.py.

13.41.4.2 rpki.async.gc_summary.threshold

Definition at line 382 of file async.py.

13.41.4.3 rpki.async.gc_summary.timer

Definition at line 382 of file async.py.

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

- [async.py \(3793\)](#)

13.42 rpki.async.iterator Class Reference

Inheritance diagram for rpki.async.iterator:

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](#)

13.42.1 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.

13.42.2 Constructor & Destructor Documentation

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

Definition at line 45 of file async.py.

13.42.3 Member Function Documentation

13.42.3.1 `def rpki.async.iterator.__call__(self)`

Definition at line 64 of file async.py.

13.42.3.2 `def rpki.async.iterator.__repr__(self)`

Definition at line 59 of file async.py.

13.42.3.3 `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.

13.42.4 Member Data Documentation

13.42.4.1 rpki.async.iterator.caller_function

Definition at line 45 of file async.py.

13.42.4.2 rpki.async.iterator.done_callback

Definition at line 45 of file async.py.

13.42.4.3 rpki.async.iterator.item_callback

Definition at line 45 of file async.py.

13.42.4.4 rpki.async.iterator.iterator

Definition at line 45 of file async.py.

13.42.4.5 rpki.async.iterator.unwind_stack

Definition at line 45 of file async.py.

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

- [async.py \(3793\)](#)

13.43 rpki.async.sync_wrapper Class Reference

Inheritance diagram for rpki.async.sync_wrapper:

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

13.43.1 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 312 of file `async.py`.

13.43.2 Constructor & Destructor Documentation

13.43.2.1 def rpki.async.sync_wrapper.__init__(self, func)

Definition at line 327 of file `async.py`.

13.43.3 Member Function Documentation

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

Definition at line 347 of file async.py.

13.43.3.2 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 330 of file async.py.

13.43.3.3 def rpki.async.sync_wrapper.eb (self, err)

Wrapped code raised an exception. Store exception data, then exit the event loop.

Definition at line 338 of file async.py.

13.43.4 Member Data Documentation

13.43.4.1 rpki.async.sync_wrapper.err = None [static]

Definition at line 325 of file async.py.

13.43.4.2 rpki.async.sync_wrapper.func

Definition at line 327 of file async.py.

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

Definition at line 324 of file async.py.

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

- [async.py \(3793\)](#)

13.44 rpki.async.timer Class Reference

Inheritance diagram for rpki.async.timer:

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.

13.44.1 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`.

13.44.2 Constructor & Destructor Documentation

13.44.2.1 `def rpki.async.timer.__init__(self, handler = None, errback = None)`

Definition at line 109 of file `async.py`.

13.44.2.2 `def rpki.async.timer.__del__(self)`

Definition at line 146 of file `async.py`.

13.44.3 Member Function Documentation

13.44.3.1 `def rpki.async.timer.__cmp__(self, other)`

Definition at line 142 of file `async.py`.

13.44.3.2 `def rpki.async.timer.__repr__(self)`

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

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

Cancel a timer, if it was set.

Definition at line 149 of file async.py.

13.44.3.4 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 239 of file async.py.

13.44.3.5 def rpki.async.timer.errback (*self*, *e*)

Error callback. May be overridden, or set with set_errback().

Definition at line 184 of file async.py.

13.44.3.6 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 167 of file async.py.

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

Test whether this timer is currently set.

Definition at line 161 of file async.py.

13.44.3.8 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 198 of file async.py.

13.44.3.9 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 218 of file async.py.

13.44.3.10 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.

13.44.3.11 def rpki.async.timer.set_errback (*self*, *errback*)

Set a timer's errback. Like set_handler(), for errbacks.

Definition at line 191 of file async.py.

13.44.3.12 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 174 of file `async.py`.

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

Debug logging.

Definition at line 118 of file `async.py`.

13.44.4 **Member Data Documentation**

13.44.4.1 **rpki.async.timer.errback**

Definition at line 193 of file `async.py`.

13.44.4.2 **rpki::async.timer::gc_debug = False [static]**

Verbose chatter about timers states and garbage collection.

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

13.44.4.3 **rpki.async.timer.handler**

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

13.44.4.4 **rpki::async.timer::queue = [] [static]**

Timer queue, shared by all timer instances (there can be only one queue).

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

13.44.4.5 **rpki::async.timer::run_debug = False [static]**

Verbose chatter about timers being run.

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

13.44.4.6 rpki.async.timer.when

Definition at line 109 of file async.py.

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

- [async.py \(3793\)](#)

13.45 rpki.cli.Cmd Class Reference

Inheritance diagram for rpki.cli.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](#) = "/-."

13.45.1 Detailed Description

Customized subclass of Python cmd module.

Definition at line 29 of file cli.py.

13.45.2 Constructor & Destructor Documentation

13.45.2.1 `def rpki.cli.Cmd.__init__ (self, argv = None)`

Definition at line 42 of file cli.py.

13.45.3 Member Function Documentation

13.45.3.1 `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.

13.45.3.2 `def rpki.cli.Cmd.complete_help (self, args)`

Better completion function for help command arguments.

Definition at line 119 of file cli.py.

13.45.3.3 `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.

13.45.3.4 `def rpki.cli.Cmd.do_EOF (self, arg)`

Exit program.

Definition at line 61 of file cli.py.

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

Exit program.

Definition at line 69 of file cli.py.

13.45.3.6 def rpki.cli.Cmd.emptyline (*self*)

Handle an empty line. cmd module default is to repeat the last command, which I find to be violation of the principal of least astonishment, so my preference is that an empty line does nothing.

Definition at line 77 of file cli.py.

13.45.3.7 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.

13.45.3.8 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.

13.45.3.9 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.

13.45.4 Member Data Documentation

13.45.4.1 `rpki.cli.Cmd.cmdloop_with_history = cmd.Cmd.cmdloop` [static]

Definition at line 153 of file cli.py.

13.45.4.2 `rpki.cli.Cmd.do_quit = do_exit` [static]

Definition at line 75 of file cli.py.

13.45.4.3 `rpki.cli.Cmd.emptyline_repeats_last_command = False` [static]

Definition at line 34 of file cli.py.

13.45.4.4 `rpki.cli.Cmd.EOF_exits_command_loop = True` [static]

Definition at line 36 of file cli.py.

13.45.4.5 `rpki.cli.Cmd.histfile = None` [static]

Reimplemented in [rpki.myrpki.main](#).

Definition at line 40 of file cli.py.

13.45.4.6 `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 \(3255\)](#)

13.46 rpki.config.parser Class Reference

Inheritance diagram for rpki.config.parser:

Collaboration diagram for rpki.config.parser:

Public Member Functions

- def [__init__](#)
- def [get](#)
- def [getboolean](#)
- def [getint](#)
- def [getlong](#)
- def [has_option](#)
- def [has_section](#)
- def [multiget](#)
- def [set_global_flags](#)

Public Attributes

- [cfg](#)
- [default_section](#)
- [filename](#)

Private Member Functions

- def [_repl](#)

Static Private Attributes

- tuple [_regexp](#) = re.compile("\\\\\${(.*?):(.*)}")

13.46.1 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.

If no filename is given to the constructor (`filename = None`), we check for an environment variable naming the config file, then we

check for a default filename in the current directory, then finally we check for a global config file if autoconf provided a directory name to check.

Definition at line 55 of file config.py.

13.46.2 Constructor & Destructor Documentation

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

Definition at line 73 of file config.py.

13.46.3 Member Function Documentation

13.46.3.1 `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 140 of file config.py.

13.46.3.2 `def rpki.config.parser.get(self, option, default = None, section = None)`

Get an option, perhaps with a default value.

Definition at line 151 of file config.py.

13.46.3.3 `def rpki.config.parser.getboolean(self, option, default = None, section = None)`

Get a boolean option, perhaps with a default value.

Definition at line 165 of file config.py.

13.46.3.4 `def rpki.config.parser.getint (self, option, default = None, section = None)`

Get an integer option, perhaps with a default value.

Definition at line 177 of file config.py.

13.46.3.5 `def rpki.config.parser.getlong (self, option, default = None, section = None)`

Get a long integer option, perhaps with a default value.

Definition at line 183 of file config.py.

13.46.3.6 `def rpki.config.parser.has_option (self, option, section = None)`

Test whether an option exists.

Definition at line 110 of file config.py.

13.46.3.7 `def rpki.config.parser.has_section (self, section)`

Test whether a section exists.

Definition at line 103 of file config.py.

13.46.3.8 `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 119 of file config.py.

13.46.3.9 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 189 of file config.py.

13.46.4 Member Data Documentation

13.46.4.1 tuple rpki.config.parser._regexp = re.compile("\\\${(.*?):?(.*)}") [static, private]

Definition at line 138 of file config.py.

13.46.4.2 rpki.config.parser.cfg

Definition at line 73 of file config.py.

13.46.4.3 rpki.config.parser.default_section

Definition at line 73 of file config.py.

13.46.4.4 rpki.config.parser.filename

Definition at line 73 of file config.py.

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

- [config.py \(3620\)](#)

13.47 rpki.exceptions.BadClassNameSyntax Class Reference

Inheritance diagram for rpki.exceptions.BadClassNameSyntax:

Collaboration diagram for rpki.exceptions.BadClassNameSyntax:

13.47.1 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 \(3465\)](#)

13.48 rpki.exceptions.BadClientURL Class Reference

Inheritance diagram for rpki.exceptions.BadClientURL:

Collaboration diagram for rpki.exceptions.BadClientURL:

13.48.1 Detailed Description

URL given to HTTP 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 \(3465\)](#)

13.49 rpki.exceptions.BadContactURL Class Reference

Inheritance diagram for rpki.exceptions.BadContactURL:

Collaboration diagram for rpki.exceptions.BadContactURL:

13.49.1 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 \(3465\)](#)

13.50 rpki.exceptions.BadExtension Class Reference

Inheritance diagram for rpki.exceptions.BadExtension:

Collaboration diagram for rpki.exceptions.BadExtension:

13.50.1 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 \(3465\)](#)

13.51 rpki.exceptions.BadIPResource Class Reference

Inheritance diagram for rpki.exceptions.BadIPResource:

Collaboration diagram for rpki.exceptions.BadIPResource:

13.51.1 Detailed Description

Parse failure for alleged IP resource string.

Definition at line 315 of file exceptions.py.

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

- [exceptions.py \(3465\)](#)

13.52 rpki.exceptions.BadIRDBReply Class Reference

Inheritance diagram for rpki.exceptions.BadIRDBReply:

Collaboration diagram for rpki.exceptions.BadIRDBReply:

13.52.1 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 \(3465\)](#)

13.53 **rpki.exceptions.BadIssueResponse Class Reference**

Inheritance diagram for `rpki.exceptions.BadIssueResponse`:

Collaboration diagram for `rpki.exceptions.BadIssueResponse`:

13.53.1 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 \(3465\)](#)

13.54 **rpki.exceptions.BadPKCS10 Class Reference**

Inheritance diagram for `rpki.exceptions.BadPKCS10`:

Collaboration diagram for `rpki.exceptions.BadPKCS10`:

13.54.1 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 \(3465\)](#)

13.55 **rpki.exceptions.BadPublicationReply Class Reference**

Inheritance diagram for `rpki.exceptions.BadPublicationReply`:

Collaboration diagram for `rpki.exceptions.BadPublicationReply`:

13.55.1 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 \(3465\)](#)

13.56 rpki.exceptions.BadQuery Class Reference

Inheritance diagram for rpki.exceptions.BadQuery:

Collaboration diagram for rpki.exceptions.BadQuery:

13.56.1 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 \(3465\)](#)

13.57 rpki.exceptions.BadROAPrefix Class Reference

Inheritance diagram for rpki.exceptions.BadROAPrefix:

Collaboration diagram for rpki.exceptions.BadROAPrefix:

13.57.1 Detailed Description

Parse failure for alleged ROA prefix string.

Definition at line 320 of file exceptions.py.

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

- [exceptions.py \(3465\)](#)

13.58 rpki.exceptions.BadSender Class Reference

Inheritance diagram for rpki.exceptions.BadSender:

Collaboration diagram for rpki.exceptions.BadSender:

13.58.1 Detailed Description

`Unexpected XML sender value.`

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

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

- [exceptions.py \(3465\)](#)

13.59 `rpki.exceptions.BadStatusCode` Class Reference

Inheritance diagram for `rpki.exceptions.BadStatusCode`:

Collaboration diagram for `rpki.exceptions.BadStatusCode`:

13.59.1 Detailed Description

`Unrecognized protocol status code.`

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

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

- [exceptions.py \(3465\)](#)

13.60 `rpki.exceptions.BadURISyntax` Class Reference

Inheritance diagram for `rpki.exceptions.BadURISyntax`:

Collaboration diagram for `rpki.exceptions.BadURISyntax`:

13.60.1 Detailed Description

`Illegal syntax for a URI.`

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

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

- [exceptions.py \(3465\)](#)

13.61 rpki.exceptions.BSCNotFound Class Reference

Inheritance diagram for rpki.exceptions.BSCNotFound:

Collaboration diagram for rpki.exceptions.BSCNotFound:

13.61.1 Detailed Description

Could not find specified BSC in database.

Definition at line 122 of file exceptions.py.

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

- [exceptions.py \(3465\)](#)

13.62 rpki.exceptions.BSCNotReady Class Reference

Inheritance diagram for rpki.exceptions.BSCNotReady:

Collaboration diagram for rpki.exceptions.BSCNotReady:

13.62.1 Detailed Description

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

Definition at line 277 of file exceptions.py.

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

- [exceptions.py \(3465\)](#)

13.63 rpki.exceptions.ChildNotFound Class Reference

Inheritance diagram for rpki.exceptions.ChildNotFound:

Collaboration diagram for rpki.exceptions.ChildNotFound:

13.63.1 Detailed Description

Could not find specified child in database.

Definition at line 117 of file exceptions.py.

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

- [exceptions.py \(3465\)](#)

13.64 rpki.exceptions.ClassNameMismatch Class Reference

Inheritance diagram for rpki.exceptions.ClassNameMismatch:

Collaboration diagram for rpki.exceptions.ClassNameMismatch:

13.64.1 Detailed Description

`class_name` does not match child context.

Definition at line 132 of file exceptions.py.

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

- [exceptions.py \(3465\)](#)

13.65 rpki.exceptions.ClassNameUnknown Class Reference

Inheritance diagram for rpki.exceptions.ClassNameUnknown:

Collaboration diagram for rpki.exceptions.ClassNameUnknown:

13.65.1 Detailed Description

Unknown `class_name`.

Definition at line 137 of file exceptions.py.

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

- [exceptions.py \(3465\)](#)

13.66 rpki.exceptions.ClientNotFound Class Reference

Inheritance diagram for rpki.exceptions.ClientNotFound:

Collaboration diagram for rpki.exceptions.ClientNotFound:

13.66.1 Detailed Description

Could not find specified client in database.

Definition at line 237 of file exceptions.py.

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

- [exceptions.py \(3465\)](#)

13.67 rpki.exceptions.CMSContentNotSet Class Reference

Inheritance diagram for rpki.exceptions.CMSContentNotSet:

Collaboration diagram for rpki.exceptions.CMSContentNotSet:

13.67.1 Detailed Description

Inner content of a CMS_object has not been set. If object is known to be valid, the .extract() method should be able to set the content; otherwise, only the .verify() method (which checks signatures) is safe.

Definition at line 302 of file exceptions.py.

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

- [exceptions.py \(3465\)](#)

13.68 rpki.exceptions.CMSCRLNotSet Class Reference

Inheritance diagram for rpki.exceptions.CMSCRLNotSet:

Collaboration diagram for rpki.exceptions.CMSCRLNotSet:

13.68.1 Detailed Description

CMS CRL has not been configured.

Definition at line 217 of file exceptions.py.

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

- [exceptions.py \(3465\)](#)

13.69 rpki.exceptions.CMSVerificationFailed Class Reference

Inheritance diagram for rpki.exceptions.CMSVerificationFailed:

Collaboration diagram for rpki.exceptions.CMSVerificationFailed:

13.69.1 Detailed Description

Verification of a CMS message failed.

Definition at line 66 of file exceptions.py.

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

- [exceptions.py \(3465\)](#)

13.70 rpki.exceptions.CommandParseFailure Class Reference

Inheritance diagram for rpki.exceptions.CommandParseFailure:

Collaboration diagram for rpki.exceptions.CommandParseFailure:

13.70.1 Detailed Description

Failed to parse command line.

Definition at line 325 of file exceptions.py.

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

- [exceptions.py \(3465\)](#)

13.71 rpki.exceptions.DBConsistencyError Class Reference

Inheritance diagram for rpki.exceptions.DBConsistencyError:

Collaboration diagram for rpki.exceptions.DBConsistencyError:

13.71.1 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 \(3465\)](#)

13.72 rpki.exceptions.DERObjectConversionError Class Reference

Inheritance diagram for rpki.exceptions.DERObjectConversionError:

Collaboration diagram for rpki.exceptions.DERObjectConversionError:

13.72.1 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 \(3465\)](#)

13.73 rpki.exceptions.DuplicateObject Class Reference

Inheritance diagram for rpki.exceptions.DuplicateObject:

Collaboration diagram for rpki.exceptions.DuplicateObject:

13.73.1 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 \(3465\)](#)

13.74 rpki.exceptions.EmptyPEM Class Reference

Inheritance diagram for rpki.exceptions.EmptyPEM:

Collaboration diagram for rpki.exceptions.EmptyPEM:

13.74.1 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 \(3465\)](#)

13.75 rpki.exceptions.EmptyROAPrefixList Class Reference

Inheritance diagram for rpki.exceptions.EmptyROAPrefixList:

Collaboration diagram for rpki.exceptions.EmptyROAPrefixList:

13.75.1 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 \(3465\)](#)

13.76 rpki.exceptions.ForbiddenURI Class Reference

Inheritance diagram for rpki.exceptions.ForbiddenURI:

Collaboration diagram for rpki.exceptions.ForbiddenURI:

13.76.1 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 \(3465\)](#)

13.77 rpki.exceptions.HandleTranslationError Class Reference

Inheritance diagram for rpki.exceptions.HandleTranslationError:

Collaboration diagram for rpki.exceptions.HandleTranslationError:

13.77.1 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 \(3465\)](#)

13.78 rpki.exceptions.HTTPBadVersion Class Reference

Inheritance diagram for rpki.exceptions.HTTPBadVersion:

Collaboration diagram for rpki.exceptions.HTTPBadVersion:

13.78.1 Detailed Description

```
HTTP 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 \(3465\)](#)

13.79 rpki.exceptions.HTTPClientAborted Class Reference

Inheritance diagram for rpki.exceptions.HTTPClientAborted:

Collaboration diagram for rpki.exceptions.HTTPClientAborted:

13.79.1 Detailed Description

```
HTTP 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 \(3465\)](#)

13.80 rpki.exceptions.HTTPRequestFailed Class Reference

Inheritance diagram for rpki.exceptions.HTTPRequestFailed:

Collaboration diagram for rpki.exceptions.HTTPRequestFailed:

13.80.1 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 \(3465\)](#)

13.81 rpki.exceptions.HTTPTimeout Class Reference

Inheritance diagram for rpki.exceptions.HTTPTimeout:

Collaboration diagram for rpki.exceptions.HTTPTimeout:

13.81.1 Detailed Description

`HTTP connection timed out.`

Definition at line 310 of file exceptions.py.

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

- [exceptions.py \(3465\)](#)

13.82 rpki.exceptions.HTTPUnexpectedState Class Reference

Inheritance diagram for rpki.exceptions.HTTPUnexpectedState:

Collaboration diagram for rpki.exceptions.HTTPUnexpectedState:

13.82.1 Detailed Description

`HTTP 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 \(3465\)](#)

13.83 rpki.exceptions.MissingCMSCRL Class Reference

Inheritance diagram for rpki.exceptions.MissingCMSCRL:

Collaboration diagram for rpki.exceptions.MissingCMSCRL:

13.83.1 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 \(3465\)](#)

13.84 rpki.exceptions.MissingCMSEECert Class Reference

Inheritance diagram for rpki.exceptions.MissingCMSEECert:

Collaboration diagram for rpki.exceptions.MissingCMSEECert:

13.84.1 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 \(3465\)](#)

13.85 rpki.exceptions.MultipleTLSEECert Class Reference

Inheritance diagram for rpki.exceptions.MultipleTLSEECert:

Collaboration diagram for rpki.exceptions.MultipleTLSEECert:

13.85.1 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 \(3465\)](#)

13.86 rpki.exceptions.MustBePrefix Class Reference

Inheritance diagram for rpki.exceptions.MustBePrefix:

Collaboration diagram for rpki.exceptions.MustBePrefix:

13.86.1 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 \(3465\)](#)

13.87 rpki.exceptions.NoActiveCA Class Reference

Inheritance diagram for rpki.exceptions.NoActiveCA:

Collaboration diagram for rpki.exceptions.NoActiveCA:

13.87.1 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 \(3465\)](#)

13.88 rpki.exceptions.NoCoveringCertForROA Class Reference

Inheritance diagram for rpki.exceptions.NoCoveringCertForROA:

Collaboration diagram for rpki.exceptions.NoCoveringCertForROA:

13.88.1 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 \(3465\)](#)

13.89 rpki.exceptions.NoObjectAtURI Class Reference

Inheritance diagram for rpki.exceptions.NoObjectAtURI:

Collaboration diagram for rpki.exceptions.NoObjectAtURI:

13.89.1 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 \(3465\)](#)

13.90 rpki.exceptions.NotACertificateChain Class Reference

Inheritance diagram for rpki.exceptions.NotACertificateChain:

Collaboration diagram for rpki.exceptions.NotACertificateChain:

13.90.1 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 \(3465\)](#)

13.91 rpki.exceptions.NotFound Class Reference

Inheritance diagram for rpki.exceptions.NotFound:

Collaboration diagram for rpki.exceptions.NotFound:

13.91.1 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 \(3465\)](#)

13.92 rpki.exceptions.NotImplementedYet Class Reference

Inheritance diagram for rpki.exceptions.NotImplementedYet:

Collaboration diagram for rpki.exceptions.NotImplementedYet:

13.92.1 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 \(3465\)](#)

13.93 rpki.exceptions.NotInDatabase Class Reference

Inheritance diagram for rpki.exceptions.NotInDatabase:

Collaboration diagram for rpki.exceptions.NotInDatabase:

13.93.1 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 \(3465\)](#)

13.94 rpki.exceptions.ReceivedTLSCACert Class Reference

Inheritance diagram for rpki.exceptions.ReceivedTLSCACert:

Collaboration diagram for rpki.exceptions.ReceivedTLSCACert:

13.94.1 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 \(3465\)](#)

13.95 rpki.exceptions.RPKI_Exception Class Reference

Inherits [Exception](#).

Inherited by [rpki.exceptions.BadClassNameSyntax](#), [rpki.exceptions.BadClientURL](#), [rpki.exceptions.BadContactURL](#), [rpki.exceptions.BadExtension](#), [rpki.exceptions.BadIPResource](#), [rpki.exceptions.BadIRDBReply](#), [rpki.exceptions.BadIssueResponse](#), [rpki.exceptions.BadPKCS10](#), [rpki.exceptions.BadPublicationReply](#), [rpki.exceptions.BadQuery](#), [rpki.exceptions.BadROAPrefix](#), [rpki.exceptions.BadSender](#), [rpki.exceptions.BadStatusCode](#), [rpki.exceptions.BadURISyntax](#), [rpki.exceptions.BSCNotFound](#), [rpki.exceptions.BSCNotReady](#), [rpki.exceptions.ChildNotFound](#), [rpki.exceptions.ClassNameMismatch](#), [rpki.exceptions.ClassNameUnknown](#), [rpki.exceptions.ClientNotFound](#), [rpki.exceptions.CMSContentNotSet](#), [rpki.exceptions.CMSCRLNotSet](#), [rpki.exceptions.CMSVerificationFailed](#), [rpki.exceptions.CommandParseFailure](#), [rpki.exceptions.DBConsistencyError](#), [rpki.exceptions.DERObjectConversionError](#), [rpki.exceptions.DuplicateObject](#), [rpki.exceptions.EmptyPEM](#), [rpki.exceptions.EmptyROAPrefixList](#), [rpki.exceptions.ForbiddenURI](#), [rpki.exceptions.HandleTranslationError](#), [rpki.exceptions.HTTPBadVersion](#), [rpki.exceptions.HTTPClientAborted](#), [rpki.exceptions.HTTPRequestFailed](#), [rpki.exceptions.HTTPTimeout](#), [rpki.exceptions.HTTPUnexpectedState](#), [rpki.exceptions.MissingCMSCRL](#), [rpki.exceptions.MissingCMSEecert](#), [rpki.exceptions.MustBePrefix](#), [rpki.exceptions.NoActiveCA](#), [rpki.exceptions.NoCoveringCertForROA](#), [rpki.exceptions.NoObjectAtURI](#), [rpki.exceptions.NotACertificateChain](#), [rpki.exceptions.NotFound](#), [rpki.exceptions.NotImplementedYet](#), [rpki.exceptions.NotInDatabase](#), [rpki.exceptions.ServerShuttingDown](#), [rpki.exceptions.SKIMismatch](#), [rpki.exceptions.SubprocessError](#), [rpki.exceptions.TLSValidationError](#), [rpki.exceptions.UnexpectedCMSCerts](#), [rpki.exceptions.UnexpectedCMSCRLs](#), [rpki.exceptions.UnparsableCMSDER](#), [rpki.exceptions.UpstreamError](#), and [rpki.exceptions.WrongEContentType](#).

Collaboration diagram for rpki.exceptions.RPKI_Exception:

13.95.1 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 \(3465\)](#)

13.96 rpki.exceptions.ServerShuttingDown Class Reference

Inheritance diagram for rpki.exceptions.ServerShuttingDown:

Collaboration diagram for rpki.exceptions.ServerShuttingDown:

13.96.1 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 \(3465\)](#)

13.97 rpki.exceptions.SKIMismatch Class Reference

Inheritance diagram for rpki.exceptions.SKIMismatch:

Collaboration diagram for rpki.exceptions.SKIMismatch:

13.97.1 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 \(3465\)](#)

13.98 rpki.exceptions.SubprocessError Class Reference

Inheritance diagram for rpki.exceptions.SubprocessError:

Collaboration diagram for rpki.exceptions.SubprocessError:

13.98.1 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 \(3465\)](#)

13.99 rpki.exceptions.TLSValidationError Class Reference

Inheritance diagram for rpki.exceptions.TLSValidationError:

Collaboration diagram for rpki.exceptions.TLSValidationError:

13.99.1 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 \(3465\)](#)

13.100 rpki.exceptions.UnexpectedCMSCerts Class Reference

Inheritance diagram for rpki.exceptions.UnexpectedCMSCerts:

Collaboration diagram for rpki.exceptions.UnexpectedCMSCerts:

13.100.1 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 \(3465\)](#)

13.101 **rpki.exceptions.UnexpectedCMSCRLs Class Reference**

Inheritance diagram for `rpki.exceptions.UnexpectedCMSCRLs`:

Collaboration diagram for `rpki.exceptions.UnexpectedCMSCRLs`:

13.101.1 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 \(3465\)](#)

13.102 **rpki.exceptions.UnparsableCMSDER Class Reference**

Inheritance diagram for `rpki.exceptions.UnparsableCMSDER`:

Collaboration diagram for `rpki.exceptions.UnparsableCMSDER`:

13.102.1 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 \(3465\)](#)

13.103 **rpki.exceptions.UpstreamError Class Reference**

Inheritance diagram for `rpki.exceptions.UpstreamError`:

Collaboration diagram for `rpki.exceptions.UpstreamError`:

13.103.1 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 \(3465\)](#)

13.104 rpki.exceptions.WrongEContentType Class Reference

Inheritance diagram for rpki.exceptions.WrongEContentType:

Collaboration diagram for rpki.exceptions.WrongEContentType:

13.104.1 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 \(3465\)](#)

13.105 rpki.http.caller Class Reference

Inheritance diagram for rpki.http.caller:

Collaboration diagram for rpki.http.caller:

Public Member Functions

- [def __call__](#)
- [def __init__](#)

Public Attributes

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

Static Public Attributes

- [debug](#) = False

13.105.1 Detailed Description

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

Definition at line 1003 of file http.py.

13.105.2 Constructor & Destructor Documentation

13.105.2.1 `def rpki.http.caller.__init__(self, proto, client_key, client_cert, server_ta, server_cert, url, debug = None)`

Definition at line 1012 of file http.py.

13.105.3 Member Function Documentation

13.105.3.1 `def rpki.http.caller.__call__(self, cb, eb, pdus)`

Definition at line 1022 of file http.py.

13.105.4 Member Data Documentation

13.105.4.1 `rpki.http.caller.client_cert`

Definition at line 1012 of file http.py.

13.105.4.2 `rpki.http.caller.client_key`

Definition at line 1012 of file http.py.

13.105.4.3 `rpki.http.caller.debug = False [static]`

Definition at line 1010 of file http.py.

13.105.4.4 rpki.http.caller.proto

Definition at line 1012 of file http.py.

13.105.4.5 rpki.http.caller.server_cert

Definition at line 1012 of file http.py.

13.105.4.6 rpki.http.caller.server_ta

Definition at line 1012 of file http.py.

13.105.4.7 rpki.http.caller.url

Definition at line 1012 of file http.py.

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

- [http.py \(3793\)](#)

13.106 rpki.http.http_client Class Reference

Inheritance diagram for rpki.http.http_client:

Collaboration diagram for rpki.http.http_client:

Public Member Functions

- def [__init__](#)
- def [dns_error](#)
- def [gotaddrinfo](#)
- 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](#)

Public Attributes

- [addr](#)
- [address](#)
- [expect_close](#)
- [host](#)
- [port](#)
- [queue](#)

Static Public Attributes

- [parse_type](#) = [http_response](#)
Stream parser should look for incoming HTTP response messages.
- [state](#) = None
Application layer connection state.
- [timeout](#) = [default_client_timeout](#)
Use the default client timeout value set in the module header.

13.106.1 Detailed Description

HTTP client stream.

Definition at line 642 of file http.py.

13.106.2 Constructor & Destructor Documentation

13.106.2.1 def rpki.http.http_client.__init__(self, queue, hostport)

Definition at line 659 of file http.py.

13.106.3 Member Function Documentation

13.106.3.1 def rpki.http.http_client.dns_error (self, e)

Handle DNS lookup errors. For now, just whack the connection. Undoubtedly we should do something better with diagnostics here.

Definition at line 684 of file http.py.

13.106.3.2 def rpki.http.http_client.gotaddrinfo (self, addinfo)

Got address data from DNS, create socket and request connection.

Definition at line 691 of file http.py.

13.106.3.3 def rpki.http.http_client.handle_close (self)

Asyncore signaled connection close. If we were waiting for that to find the end of a response message, process the resulting message now; if we were waiting for the response to a request we sent, signal the error.

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

Definition at line 778 of file http.py.

13.106.3.4 def rpki.http.http_client.handle_connect (self)

Asyncore says socket has connected.

Definition at line 707 of file http.py.

13.106.3.5 def rpki.http.http_client.handle_error (self)

Asyncore says something threw an exception. Log it, then shut down the connection and pass back the exception.

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

Definition at line 808 of file http.py.

13.106.3.6 def rpki.http.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 743 of file http.py.

13.106.3.7 def rpki.http.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 723 of file http.py.

13.106.3.8 def rpki.http.http_client.handle_timeout (*self*)

Connection idle timer has expired. Shut down connection in any case, noisily if we weren't idle.

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

Definition at line 794 of file http.py.

13.106.3.9 def rpki.http.http_client.send_request (*self*, *msg*)

Queue up request message and kickstart connection.

Definition at line 732 of file http.py.

13.106.3.10 def rpki.http.http_client.set_state (*self*, *state*)

Set HTTP client connection state.

Definition at line 716 of file http.py.

13.106.3.11 def rpki.http.http_client.start (*self*)

Create socket and request a connection.

Definition at line 668 of file http.py.

13.106.4 Member Data Documentation**13.106.4.1 rpki.http.http_client.addr**

Definition at line 693 of file http.py.

13.106.4.2 rpki.http.http_client.address

Definition at line 693 of file http.py.

13.106.4.3 rpki.http.http_client.expect_close

Definition at line 659 of file http.py.

13.106.4.4 rpki.http.http_client.host

Definition at line 659 of file http.py.

13.106.4.5 rpki::http.http_client::parse_type = http_response [static]

Stream parser should look for incoming HTTP response messages.

Definition at line 649 of file http.py.

13.106.4.6 rpki.http.http_client.port

Definition at line 659 of file http.py.

13.106.4.7 rpki.http.http_client.queue

Definition at line 659 of file http.py.

13.106.4.8 rpki::http.http_client::state = None [static]

Application layer connection state.

Definition at line 657 of file http.py.

13.106.4.9 rpki::http.http_client::timeout = default_client_timeout [static]

Use the default client timeout value set in the module header.

Definition at line 653 of file http.py.

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

- [http.py \(3793\)](#)

13.107 rpki.http.http_listener Class Reference

Inheritance diagram for rpki.http.http_listener:

Collaboration diagram for rpki.http.http_listener:

Public Member Functions

- [def __init__](#)
- [def __repr__](#)
- [def handle_accept](#)
- [def handle_error](#)

Public Attributes

- [handlers](#)

Static Public Attributes

- [log](#) = `log_method`
- [show_tracebacks](#) = `False`

13.107.1 Detailed Description

Listener for incoming HTTP connections.

Definition at line 579 of file `http.py`.

13.107.2 Constructor & Destructor Documentation

13.107.2.1 `def rpki.http.http_listener.__init__(self, handlers, addinfo)`

Definition at line 594 of file `http.py`.

13.107.3 Member Function Documentation

13.107.3.1 `def rpki.http.http_listener.__repr__(self)`

Definition at line 587 of file `http.py`.

13.107.3.2 `def rpki.http.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 data.

Definition at line 617 of file http.py.

13.107.3.3 def rpki.http.http_listener.handle_error (self)

Asyncore signaled an error, pass it along or log it.

Definition at line 632 of file http.py.

13.107.4 Member Data Documentation

13.107.4.1 rpki.http.http_listener.handlers

Definition at line 594 of file http.py.

13.107.4.2 rpki.http.http_listener.log = log_method [static]

Definition at line 584 of file http.py.

13.107.4.3 rpki.http.http_listener.show_tracebacks = False [static]

Definition at line 585 of file http.py.

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

- [http.py \(3793\)](#)

13.108 rpki.http.http_message Class Reference

Inheritance diagram for rpki.http.http_message:

Collaboration diagram for rpki.http.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"

13.108.1 Detailed Description

Virtual class representing of one HTTP message.

Definition at line 125 of file http.py.

13.108.2 Constructor & Destructor Documentation

13.108.2.1 def rpki.http.http_message.__init__(self, version = None, body = None, headers = None)

Definition at line 132 of file http.py.

13.108.3 Member Function Documentation

13.108.3.1 def rpki.http.http_message.__str__(self)

Definition at line 190 of file http.py.

13.108.3.2 def rpki.http.http_message.format (*self*)

Format an outgoing HTTP message.

Definition at line 175 of file http.py.

13.108.3.3 def rpki.http.http_message.normalize_headers (*self*, *headers* = *None*)

Clean up (some of) the horrible messes that HTTP allows in its headers.

Definition at line 138 of file http.py.

13.108.3.4 def rpki.http.http_message.parse_from_wire (*cls*, *headers*)

Parse and normalize an incoming HTTP message.

Definition at line 161 of file http.py.

13.108.3.5 def rpki.http.http_message.parse_version (*self*, *version*)

Parse HTTP version, raise an exception if we can't.

Definition at line 193 of file http.py.

13.108.3.6 def rpki.http.http_message.persistent (*self*)

Figure out whether this HTTP message encourages a persistent connection.

Definition at line 202 of file http.py.

13.108.4 Member Data Documentation

13.108.4.1 rpki.http.http_message.body

Definition at line 132 of file http.py.

13.108.4.2 rpki.http.http_message.headers

Definition at line 132 of file http.py.

13.108.4.3 string rpki.http.http_message.software_name = "ISC RPKI library" [static]

Definition at line 130 of file http.py.

13.108.4.4 rpki.http.http_message.version

Definition at line 132 of file http.py.

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

- [http.py \(3793\)](#)

13.109 rpki.http.http_queue Class Reference

Inheritance diagram for rpki.http.http_queue:

Collaboration diagram for rpki.http.http_queue:

Public Member Functions

- def [__init__](#)
- def [__repr__](#)
- def [detach](#)
- def [request](#)
- def [restart](#)
- def [return_result](#)

- def [send_request](#)

Public Attributes

- [client](#)
- [hostport](#)
- [queue](#)

Static Public Attributes

- [log](#) = `log_method`

13.109.1 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 818 of file `http.py`.

13.109.2 Constructor & Destructor Documentation

13.109.2.1 `def rpki.http.http_queue.__init__(self, hostport)`

Definition at line 830 of file `http.py`.

13.109.3 Member Function Documentation

13.109.3.1 `def rpki.http.http_queue.__repr__(self)`

Definition at line 827 of file `http.py`.

13.109.3.2 `def rpki.http.http_queue.detach(self, client_)`

Detach a client from this queue. Silently ignores attempting to detach a client that is not attached to this queue, to simplify handling of what otherwise would be a nasty set of race conditions.

Definition at line 874 of file http.py.

13.109.3.3 def rpki.http.http_queue.request (*self*, *requests*)

Append http_request object(s) to this queue.

Definition at line 836 of file http.py.

13.109.3.4 def rpki.http.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 843 of file http.py.

13.109.3.5 def rpki.http.http_queue.return_result (*self*, *client*, *result*, *detach = False*)

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 885 of file http.py.

13.109.3.6 def rpki.http.http_queue.send_request (*self*)

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

Definition at line 867 of file http.py.

13.109.4 Member Data Documentation

13.109.4.1 rpki.http.http_queue.client

Definition at line 830 of file http.py.

13.109.4.2 rpki.http.http_queue.hostport

Definition at line 830 of file http.py.

13.109.4.3 rpki.http.http_queue.log = log_method [static]

Definition at line 825 of file http.py.

13.109.4.4 rpki.http.http_queue.queue

Definition at line 830 of file http.py.

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

- [http.py \(3793\)](#)

13.110 rpki.http.http_request Class Reference

Inheritance diagram for rpki.http.http_request:

Collaboration diagram for rpki.http.http_request:

Public Member Functions

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

Public Attributes

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

13.110.1 Detailed Description

HTTP request message.

Definition at line 214 of file http.py.

13.110.2 Constructor & Destructor Documentation

13.110.2.1 `def rpki.http.http_request.__init__(self, cmd = None, path = None, version = default_http_version, body = None, callback = None, errback = None, headers)`

Definition at line 219 of file http.py.

13.110.3 Member Function Documentation

13.110.3.1 `def rpki.http.http_request.__repr__(self)`

Definition at line 244 of file http.py.

13.110.3.2 `def rpki.http.http_request.format_first_line(self)`

Format first line of HTTP request message, and set up the User-Agent header.

Definition at line 236 of file http.py.

13.110.3.3 `def rpki.http.http_request.parse_first_line (self, cmd, path, version)`

Parse first line of HTTP request message.

Definition at line 228 of file http.py.

13.110.4 Member Data Documentation

13.110.4.1 `rpki.http.http_request.callback`

Definition at line 219 of file http.py.

13.110.4.2 `rpki.http.http_request.cmd`

Definition at line 219 of file http.py.

13.110.4.3 `rpki.http.http_request.errback`

Definition at line 219 of file http.py.

13.110.4.4 `rpki.http.http_request.path`

Definition at line 219 of file http.py.

13.110.4.5 `rpki.http.http_request.retried`

Definition at line 219 of file http.py.

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

- [http.py \(3793\)](#)

13.111 rpki.http.http_response Class Reference

Inheritance diagram for rpki.http.http_response:

Collaboration diagram for rpki.http.http_response:

Public Member Functions

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

Public Attributes

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

13.111.1 Detailed Description

HTTP response message.

Definition at line 247 of file http.py.

13.111.2 Constructor & Destructor Documentation

13.111.2.1 `def rpki.http.http_response.__init__(self, code = None, reason = None, version = default_http_version, body = None, headers)`

Definition at line 252 of file http.py.

13.111.3 Member Function Documentation

13.111.3.1 `def rpki.http.http_response.__repr__(self)`

Definition at line 274 of file http.py.

13.111.3.2 def rpki.http.http_response.format_first_line (self)

Format first line of HTTP response message, and set up Date and Server headers.

Definition at line 265 of file http.py.

13.111.3.3 def rpki.http.http_response.parse_first_line (self, version, code, reason)

Parse first line of HTTP response message.

Definition at line 257 of file http.py.

13.111.4 Member Data Documentation

13.111.4.1 rpki.http.http_response.code

Definition at line 252 of file http.py.

13.111.4.2 rpki.http.http_response.reason

Definition at line 252 of file http.py.

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

- [http.py \(3793\)](#)

13.112 rpki.http.http_server Class Reference

Inheritance diagram for rpki.http.http_server:

Collaboration diagram for rpki.http.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](#)

Public Attributes

- [expect_close](#)
- [handlers](#)

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.

13.112.1 Detailed Description

HTTP server stream.

Definition at line 479 of file http.py.

13.112.2 Constructor & Destructor Documentation

13.112.2.1 def rpki.http.http_server.__init__(self, sock, handlers)

Definition at line 492 of file http.py.

13.112.3 Member Function Documentation

13.112.3.1 def rpki.http.http_server.find_handler (self, path)

Helper method to search self.handlers.

Definition at line 506 of file http.py.

13.112.3.2 def rpki.http.http_server.handle_message (self)

HTTP layer 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 515 of file http.py.

13.112.3.3 def rpki.http.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 498 of file http.py.

13.112.3.4 def rpki.http.http_server.send_error (self, code, reason)

Send an error response to this request.

Definition at line 545 of file http.py.

13.112.3.5 def rpki.http.http_server.send_message (self, code, reason = "OK", body = None)

Queue up reply message. If both parties agree that connection is persistent, 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 557 of file http.py.

13.112.3.6 def rpki.http.http_server.send_reply (self, code, body = None, reason = "OK")

Send a reply to this request.

Definition at line 551 of file http.py.

13.112.4 Member Data Documentation

13.112.4.1 rpki.http.http_server.expect_close

Definition at line 492 of file http.py.

13.112.4.2 rpki.http.http_server.handlers

Definition at line 492 of file http.py.

13.112.4.3 rpki::http.http_server::parse_type = http_request [static]

Stream parser should look for incoming HTTP request messages.

Definition at line 486 of file http.py.

13.112.4.4 rpki::http.http_server::timeout = default_server_timeout [static]

Use the default server timeout value set in the module header.

Definition at line 490 of file http.py.

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

- [http.py \(3793\)](#)

13.113 rpki.http.http_stream Class Reference

Inheritance diagram for rpki.http.http_stream:

Collaboration diagram for rpki.http.http_stream:

Public Member Functions

- def [__init__](#)
- def [__repr__](#)
- def [chunk_body](#)

- def [chunk_discard_crlf](#)
- def [chunk_discard_trailer](#)
- def [chunk_header](#)
- def [collect_incoming_data](#)
- def [found_terminator](#)
- def [get_buffer](#)
- def [handle_body](#)
- def [handle_close](#)
- def [handle_error](#)
- def [handle_timeout](#)
- def [restart](#)
- def [update_timeout](#)

Public Attributes

- [buffer](#)
- [chunk_handler](#)
- [msg](#)
- [timer](#)

Static Public Attributes

- [log](#) = [log_method](#)
- [show_tracebacks](#) = False

13.113.1 Detailed Description

Virtual class representing an HTTP message stream.

Definition at line 298 of file http.py.

13.113.2 Constructor & Destructor Documentation

13.113.2.1 def rpki.http.http_stream.__init__(self, sock = None)

Definition at line 314 of file http.py.

13.113.3 Member Function Documentation

13.113.3.1 `def rpki.http.http_stream.__repr__ (self)`

Definition at line 306 of file http.py.

13.113.3.2 `def rpki.http.http_stream.chunk_body (self)`

Asynchcat 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 406 of file http.py.

13.113.3.3 `def rpki.http.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 418 of file http.py.

13.113.3.4 `def rpki.http.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 428 of file http.py.

13.113.3.5 `def rpki.http.http_stream.chunk_header (self)`

Asynchcat 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 390 of file http.py.

13.113.3.6 def rpki.http.http_stream.collect_incoming_data (*self*, *data*)

Buffer incoming data from asynchat.

Definition at line 342 of file http.py.

13.113.3.7 def rpki.http.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 357 of file http.py.

13.113.3.8 def rpki.http.http_stream.get_buffer (*self*)

Consume data buffered from asynchat.

Definition at line 349 of file http.py.

13.113.3.9 def rpki.http.http_stream.handle_body (*self*)

Hand normal (not chunked) message off to the application.

Definition at line 439 of file http.py.

13.113.3.10 def rpki.http.http_stream.handle_close (self)

Wrapper around asynchat connection close handler, so that we can log the event, cancel timer, and so forth.

Reimplemented in [rpki.http.http_client](#).

Definition at line 470 of file http.py.

13.113.3.11 def rpki.http.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.http.http_client](#).

Definition at line 446 of file http.py.

13.113.3.12 def rpki.http.http_stream.handle_timeout (self)

Inactivity timer expired, close connection with prejudice.

Reimplemented in [rpki.http.http_client](#).

Definition at line 463 of file http.py.

13.113.3.13 def rpki.http.http_stream.restart (self)

(Re)start HTTP message parser, reset timer.

Definition at line 320 of file http.py.

13.113.3.14 def rpki.http.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 329 of file http.py.

13.113.4 Member Data Documentation

13.113.4.1 rpki.http.http_stream.buffer

Definition at line 314 of file http.py.

13.113.4.2 rpki.http.http_stream.chunk_handler

Definition at line 322 of file http.py.

13.113.4.3 rpki.http.http_stream.log = log_method [static]

Definition at line 303 of file http.py.

13.113.4.4 rpki.http.http_stream.msg

Definition at line 372 of file http.py.

13.113.4.5 rpki.http.http_stream.show_tracebacks = False [static]

Definition at line 304 of file http.py.

13.113.4.6 rpki.http.http_stream.timer

Definition at line 314 of file http.py.

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

- [http.py \(3793\)](#)

13.114 rpki.ipaddrs.v4addr Class Reference

Inheritance diagram for rpki.ipaddrs.v4addr:

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

13.114.1 Detailed Description

IPv4 address.

Derived from long, but supports IPv4 print syntax.

Definition at line 47 of file ipaddrs.py.

13.114.2 Member Function Documentation

13.114.2.1 def rpki.ipaddrs.v4addr.__new__(cls, x)

Construct a v4addr object.

Definition at line 56 of file ipaddrs.py.

13.114.2.2 def rpki.ipaddrs.v4addr.__str__(self)

Convert a v4addr object to string format.

Definition at line 78 of file ipaddrs.py.

13.114.2.3 def rpki.ipaddrs.v4addr.from_bytes (cls, x)

Convert from a raw byte string to a v4addr object.

Definition at line 72 of file ipaddrs.py.

13.114.2.4 def rpki.ipaddrs.v4addr.to_bytes (self)

Convert a v4addr object to a raw byte string.

Definition at line 65 of file ipaddrs.py.

13.114.3 Member Data Documentation

13.114.3.1 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 \(3551\)](#)

13.115 rpki.ipaddrs.v6addr Class Reference

Inheritance diagram for rpki.ipaddrs.v6addr:

Collaboration diagram for rpki.ipaddrs.v6addr:

Public Member Functions

- def [__new__](#)
- def [__str__](#)
- def [from_bytes](#)
- def [to_bytes](#)

Static Public Attributes

- int [bits](#) = 128

13.115.1 Detailed Description

IPv6 address.

Derived from long, but supports IPv6 print syntax.

Definition at line 84 of file ipaddrs.py.

13.115.2 Member Function Documentation

13.115.2.1 def rpki.ipaddrs.v6addr.__new__(cls, x)

Construct a v6addr object.

Definition at line 93 of file ipaddrs.py.

13.115.2.2 def rpki.ipaddrs.v6addr.__str__(self)

Convert a v6addr object to string format.

Definition at line 116 of file ipaddrs.py.

13.115.2.3 def rpki.ipaddrs.v6addr.from_bytes(cls, x)

Convert from a raw byte string to a v6addr object.

Definition at line 109 of file ipaddrs.py.

13.115.2.4 def rpki.ipaddrs.v6addr.to_bytes(self)

Convert a v6addr object to a raw byte string.

Definition at line 102 of file ipaddrs.py.

13.115.3 Member Data Documentation

13.115.3.1 int rpki.ipaddrs.v6addr.bits = 128 [static]

Definition at line 91 of file ipaddrs.py.

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

- [ipaddrs.py \(3551\)](#)

13.116 rpki.irdbd.main Class Reference

Inheritance diagram for rpki.irdbd.main:

Collaboration diagram for rpki.irdbd.main:

Public Member Functions

- def [__init__](#)
- def [handle_list_ghostbuster_requests](#)
- def [handle_list_resources](#)
- def [handle_list_roa_requests](#)
- def [handler](#)

Public Attributes

- [bpki_ta](#)
- [cfg](#)
- [cur](#)
- [db](#)
- [irdbd_cert](#)
- [irdbd_key](#)
- [rpkid_cert](#)

Static Public Attributes

- dictionary [handle_dispatch](#)

13.116.1 Detailed Description

Definition at line 51 of file rpki/irdbd.py.

13.116.2 Constructor & Destructor Documentation

13.116.2.1 def rpki.irdbd.main.__init__ (*self*)

Definition at line 202 of file rpki/irdbd.py.

13.116.3 Member Function Documentation

13.116.3.1 def rpki.irdbd.main.handle_list_ghostbuster_requests (*self*, *q_pdu*, *r_msg*)

Definition at line 118 of file rpki/irdbd.py.

13.116.3.2 def rpki.irdbd.main.handle_list_resources (*self*, *q_pdu*, *r_msg*)

Definition at line 54 of file rpki/irdbd.py.

13.116.3.3 def rpki.irdbd.main.handle_list_roa_requests (*self*, *q_pdu*, *r_msg*)

Definition at line 92 of file rpki/irdbd.py.

13.116.3.4 def rpki.irdbd.main.handler (*self*, *query*, *path*, *cb*)

Definition at line 149 of file rpki/irdbd.py.

13.116.4 Member Data Documentation

13.116.4.1 rpki.irdbd.main.bpki_ta

Definition at line 202 of file rpki/irdbd.py.

13.116.4.2 rpki.irdbd.main.cfg

Definition at line 202 of file rpki/irdbd.py.

13.116.4.3 rpki.irdbd.main.cur

Definition at line 202 of file rpki/irdbd.py.

13.116.4.4 rpki.irdbd.main.db

Definition at line 202 of file rpki/irdbd.py.

13.116.4.5 dictionary rpki.irdbd.main.handle_dispatch [static]

Initial value:

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

Definition at line 143 of file rpki/irdbd.py.

13.116.4.6 rpki.irdbd.main.irdbd_cert

Definition at line 202 of file rpki/irdbd.py.

13.116.4.7 rpki.irdbd.main.irdbd_key

Definition at line 202 of file rpki/irdbd.py.

13.116.4.8 rpki.irdbd.main.rpkid_cert

Definition at line 202 of file rpki/irdbd.py.

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

- [rpki/irdbd.py \(3793\)](#)

13.117 rpki.left_right.bsc_elt Class Reference

Inheritance diagram for rpki.left_right.bsc_elt:

Collaboration diagram for rpki.left_right.bsc_elt:

Public Member Functions

- def [children](#)
- def [parents](#)
- def [repositories](#)
- def [serve_pre_save_hook](#)

Static Public Attributes

- tuple [attributes](#) = ("action", "tag", "[self_handle](#)", "bsc_handle", "key_type", "hash_alg", "key_length")
XML attributes for this element.
- tuple [booleans](#) = ("generate_keypair",)
Boolean attributes (value "yes" or "no") for this element.
- string [element_name](#) = "bsc"
- tuple [elements](#) = ("signing_cert", "[signing_cert_crl](#)", "[pkcs10_request](#)")
XML elements contained by this element.
- tuple [handles](#) = (("self", self_elt),)
- [pkcs10_request](#) = None
- [private_key_id](#) = None
- [signing_cert](#) = None
- [signing_cert_crl](#) = None
- tuple [sql_template](#)

13.117.1 Detailed Description

<bsc/> (Business Signing Context) element.

Definition at line 705 of file left_right.py.

13.117.2 Member Function Documentation

13.117.2.1 def rpki.left_right.bsc_elt.children (*self*)

Fetch all child objects that link to this BSC object.

Definition at line 743 of file left_right.py.

13.117.2.2 def rpki.left_right.bsc_elt.parents (*self*)

Fetch all parent objects that link to this BSC object.

Definition at line 736 of file left_right.py.

13.117.2.3 def rpki.left_right.bsc_elt.repositories (*self*)

Fetch all repository objects that link to this BSC object.

Definition at line 729 of file left_right.py.

13.117.2.4 def rpki.left_right.bsc_elt.serve_pre_save_hook (*self*, *q_pdu*, *r_pdu*, *cb*, *eb*)

Extra server actions for bsc_elt -- handle key generation. For now this only allows RSA with SHA-256.

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

Definition at line 749 of file left_right.py.

13.117.3 Member Data Documentation

13.117.3.1 tuple rpki.left_right.bsc_elt.attributes = ("action", "tag", "self_handle", "bsc_handle", "key_type", "hash_alg", "key_length") [static]

XML attributes for this element.

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

Definition at line 711 of file left_right.py.

```
13.117.3.2  tuple rpki.left_right.bsc_elt.booleans = ("generate_keypair",)
            [static]
```

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

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

Definition at line 713 of file left_right.py.

```
13.117.3.3  string rpki.left_right.bsc_elt.element_name = "bsc"  [static]
```

Definition at line 710 of file left_right.py.

```
13.117.3.4  tuple rpki.left_right.bsc_elt.elements = ("signing_cert",
            "signing_cert_crl", "pkcs10_request") [static]
```

XML elements contained by this element.

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

Definition at line 712 of file left_right.py.

```
13.117.3.5  tuple rpki.left_right.bsc_elt.handles = (("self", self_elt),)
            [static]
```

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

Definition at line 721 of file left_right.py.

```
13.117.3.6  rpki.left_right.bsc_elt.pkcs10_request = None  [static]
```

Definition at line 724 of file left_right.py.

13.117.3.7 rpki.left_right.bsc_elt.private_key_id = None [static]

Definition at line 723 of file left_right.py.

13.117.3.8 rpki.left_right.bsc_elt.signing_cert = None [static]

Reimplemented in [irbe_cli.bsc_elt](#).

Definition at line 725 of file left_right.py.

13.117.3.9 rpki.left_right.bsc_elt.signing_cert_crl = None [static]

Reimplemented in [irbe_cli.bsc_elt](#).

Definition at line 726 of file left_right.py.

13.117.3.10 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 715 of file left_right.py.

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

- [left_right.py \(3793\)](#)

13.118 rpki.left_right.child_elt Class Reference

Inheritance diagram for rpki.left_right.child_elt:

Collaboration diagram for rpki.left_right.child_elt:

Public Member Functions

- def [ca_from_class_name](#)

- def [child_certs](#)
- def [fetch_child_certs](#)
- def [parents](#)
- def [serve_destroy_hook](#)
- def [serve_post_save_hook](#)
- def [serve_reissue](#)
- def [serve_up_down](#)

Static Public Attributes

- tuple [attributes](#) = ("action", "tag", "[self_handle](#)", "child_handle", "bsc_handle")

XML attributes for this element.

- tuple [booleans](#) = ("reissue",)

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

- [bpki_cert](#) = None
- [bpki_glue](#) = None
- 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](#)

13.118.1 Detailed Description

<child/> element.

Definition at line 1016 of file left_right.py.

13.118.2 Member Function Documentation

13.118.2.1 def rpki.left_right.child_elt.ca_from_class_name (self, class_name)

Fetch the CA corresponding to an up-down class_name.

Definition at line 1075 of file left_right.py.

13.118.2.2 `def rpki.left_right.child_elt.child_certs (self)`

Fetch all `child_cert` objects that link to this `child` object.

Definition at line 1044 of file `left_right.py`.

13.118.2.3 `def rpki.left_right.child_elt.fetch_child_certs (self, ca_detail = None, ski = None, unique = False)`

Fetch all `child_cert` objects that link to this `child` object.

Definition at line 1037 of file `left_right.py`.

13.118.2.4 `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 1051 of file `left_right.py`.

13.118.2.5 `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 1089 of file `left_right.py`.

13.118.2.6 `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 1057 of file `left_right.py`.

13.118.2.7 `def rpki.left_right.child_elt.serve_reissue (self, cb, eb)`

Handle a left-right reissue action for this child.

Definition at line 1066 of file left_right.py.

13.118.2.8 `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 1099 of file left_right.py.

13.118.3 Member Data Documentation**13.118.3.1** `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 1022 of file left_right.py.

13.118.3.2 `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 1024 of file left_right.py.

13.118.3.3 `rpki.left_right.child_elt.bpki_cert = None [static]`

Definition at line 1034 of file left_right.py.

13.118.3.4 rpki.left_right.child_elt.bpki_glue = None [static]

Definition at line 1035 of file left_right.py.

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

Definition at line 1021 of file left_right.py.

13.118.3.6 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 1023 of file left_right.py.

13.118.3.7 tuple rpki.left_right.child_elt.handles = ("self", self_elt), ("bsc", bsc_elt) [static]

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

Definition at line 1032 of file left_right.py.

13.118.3.8 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),
                  ("last_cms_timestamp", rpki.sundial.datetime))
```

Definition at line 1026 of file left_right.py.

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

- [left_right.py \(3793\)](#)

13.119 rpki.left_right.cms_msg Class Reference

Inheritance diagram for rpki.left_right.cms_msg:

Collaboration diagram for rpki.left_right.cms_msg:

Static Public Attributes

- string [encoding](#) = "us-ascii"
- [saxify](#) = sax_handler.saxify
- [schema](#) = [rpki.relaxng.left_right](#)

13.119.1 Detailed Description

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

Definition at line 1360 of file left_right.py.

13.119.2 Member Data Documentation

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

Definition at line 1365 of file left_right.py.

13.119.2.2 rpki.left_right.cms_msg.saxify = sax_handler.saxify [static]

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

Definition at line 1367 of file left_right.py.

13.119.2.3 rpki.left_right.cms_msg.schema = rpki.relaxng.left_right [static]

Definition at line 1366 of file left_right.py.

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

- [left_right.py \(3793\)](#)

13.120 rpki.left_right.data_elt Class Reference

Inheritance diagram for rpki.left_right.data_elt:

Collaboration diagram for rpki.left_right.data_elt:

Public Member Functions

- def [bsc](#)
- def [make_reply_clone_hook](#)
- def [self](#)
- def [serve_fetch_all](#)
- def [serve_fetch_handle](#)
- def [serve_fetch_one_maybe](#)
- def [serve_pre_save_hook](#)

Static Public Attributes

- tuple [handles](#) = ()
- [self_handle](#) = None
- [self_id](#) = None

13.120.1 Detailed Description

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

Definition at line 50 of file left_right.py.

13.120.2 Member Function Documentation

13.120.2.1 def rpki.left_right.data_elt.bsc (self)

Return BSC object to which this object links.

Definition at line 68 of file left_right.py.

13.120.2.2 def rpki.left_right.data_elt.make_reply_clone_hook (self, r_pdu)

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

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

Definition at line 74 of file left_right.py.

13.120.2.3 def rpki.left_right.data_elt.self (*self*)

Fetch self object to which this object links.

Definition at line 61 of file left_right.py.

13.120.2.4 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 105 of file left_right.py.

13.120.2.5 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 90 of file left_right.py.

13.120.2.6 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 96 of file left_right.py.

13.120.2.7 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 112 of file left_right.py.

13.120.3 Member Data Documentation

13.120.3.1 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.

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

Definition at line 58 of file left_right.py.

13.120.3.3 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 \(3793\)](#)

13.121 rpki.left_right.left_right_namespace Class Reference

Inheritance diagram for rpki.left_right.left_right_namespace:

Collaboration diagram for rpki.left_right.left_right_namespace:

Static Public Attributes

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

13.121.1 Detailed Description

XML namespace parameters for left-right protocol.

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

13.121.2 Member Data Documentation

13.121.2.1 dictionary `rpki.left_right.left_right_namespace.nsmap` = { None : `xmlns` } [static]

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

13.121.2.2 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 \(3793\)](#)

13.122 rpki.left_right.list_ghostbuster_requests_elt Class Reference

Inheritance diagram for `rpki.left_right.list_ghostbuster_requests_elt`:

Collaboration diagram for `rpki.left_right.list_ghostbuster_requests_elt`:

Static Public Attributes

- tuple `attributes` = ("self_handle", "tag", "parent_handle")
XML attributes for this element.

- string `element_name` = "list_ghostbuster_requests"
- string `text_attribute` = "vcard"
Name of the class attribute that holds the text value.
- `vcard` = None

13.122.1 Detailed Description

`<list_ghostbuster_requests/> element.`

Definition at line 1193 of file `left_right.py`.

13.122.2 Member Data Documentation

13.122.2.1 tuple `rpki.left_right.list_ghostbuster_requests_elt.attributes` =
("self_handle", "tag", "parent_handle") [`static`]

XML attributes for this element.

Reimplemented from `rpki.xml_utils.base_elt`.

Definition at line 1199 of file `left_right.py`.

13.122.2.2 string `rpki.left_right.list_ghostbuster_requests_elt.element_name` =
"list_ghostbuster_requests" [`static`]

Definition at line 1198 of file `left_right.py`.

13.122.2.3 string `rpki.left_right.list_ghostbuster_requests_elt.text_attribute` =
"vcard" [`static`]

Name of the class attribute that holds the text value.

Reimplemented from `rpki.xml_utils.text_elt`.

Definition at line 1200 of file `left_right.py`.

13.122.2.4 rpki.left_right.list_ghostbuster_requests_elt.vcard = None [static]

Definition at line 1202 of file left_right.py.

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

- [left_right.py \(3793\)](#)

13.123 rpki.left_right.list_published_objects_elt Class Reference

Inheritance diagram for rpki.left_right.list_published_objects_elt:

Collaboration diagram for rpki.left_right.list_published_objects_elt:

Public Member Functions

- def [make_reply](#)
- def [serve_dispatch](#)

Static Public Attributes

- tuple [attributes](#) = ("self_handle", "tag", "uri")
XML attributes for this element.
- string [element_name](#) = "list_published_objects"
- [obj](#) = None
- string [text_attribute](#) = "obj"
Name of the class attribute that holds the text value.

13.123.1 Detailed Description

<list_published_objects/> element.

Definition at line 1205 of file left_right.py.

13.123.2 Member Function Documentation

13.123.2.1 def rpki.left_right.list_published_objects_elt.make_reply (self, uri, obj)

Generate one reply PDU.

Definition at line 1233 of file left_right.py.

13.123.2.2 `def rpki.left_right.list_published_objects_elt.serve_dispatch (self, r_msg, cb, eb)`

Handle a <list_published_objects/> query. The method name is a misnomer here, there's no action attribute and no dispatch, we just dump every published object for the specified <self/> and return.

Definition at line 1216 of file left_right.py.

13.123.3 Member Data Documentation

13.123.3.1 `tuple rpki.left_right.list_published_objects_elt.attributes = ("self_handle", "tag", "uri") [static]`

XML attributes for this element.

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

Definition at line 1211 of file left_right.py.

13.123.3.2 `string rpki.left_right.list_published_objects_elt.element_name = "list_published_objects" [static]`

Definition at line 1210 of file left_right.py.

13.123.3.3 `rpki.left_right.list_published_objects_elt.obj = None [static]`

Definition at line 1214 of file left_right.py.

13.123.3.4 `string rpki.left_right.list_published_objects_elt.text_attribute = "obj" [static]`

Name of the class attribute that holds the text value.

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

Definition at line 1212 of file left_right.py.

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

- [left_right.py \(3793\)](#)

13.124 rpki.left_right.list_received_resources_elt Class Reference

Inheritance diagram for rpki.left_right.list_received_resources_elt:

Collaboration diagram for rpki.left_right.list_received_resources_elt:

Public Member Functions

- def [make_reply](#)
- def [serve_dispatch](#)

Static Public Attributes

- tuple [attributes](#)
XML attributes for this element.
- string [element_name](#) = "list_received_resources"

13.124.1 Detailed Description

`<list_received_resources/> element.`

Definition at line 1241 of file left_right.py.

13.124.2 Member Function Documentation

13.124.2.1 `def rpki.left_right.list_received_resources_elt.make_reply (self, parent_handle, uri, cert)`

Generate one reply PDU.

Definition at line 1264 of file left_right.py.

13.124.2.2 `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 1250 of file left_right.py.

13.124.3 Member Data Documentation

13.124.3.1 `tuple rpki.left_right.list_received_resources_elt.attributes [static]`

Initial value:

```
("self_handle", "tag", "parent_handle",
    "notBefore", "notAfter", "uri", "sia_uri", "aia_uri", "asn", "ipv4", "ipv6")
```

XML attributes for this element.

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

Definition at line 1247 of file left_right.py.

13.124.3.2 `string rpki.left_right.list_received_resources_elt.element_name = "list_received_resources" [static]`

Definition at line 1246 of file left_right.py.

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

- [left_right.py \(3793\)](#)

13.125 rpki.left_right.list_resources_elt Class Reference

Inheritance diagram for rpki.left_right.list_resources_elt:

Collaboration diagram for rpki.left_right.list_resources_elt:

Public Member Functions

- def [startElement](#)
- def [toXML](#)

Public Attributes

- [asn](#)
- [ipv4](#)
- [ipv6](#)

Static Public Attributes

- tuple [attributes](#) = ("self_handle", "tag", "child_handle", "[valid_until](#)", "[asn](#)", "[ipv4](#)", "[ipv6](#)")
XML attributes for this element.
- string [element_name](#) = "list_resources"
- [valid_until](#) = None

13.125.1 Detailed Description

<list_resources/> element.

Definition at line 1138 of file left_right.py.

13.125.2 Member Function Documentation

13.125.2.1 def rpki.left_right.list_resources_elt.startElement (*self*, *stack*, *name*, *attrs*)

Handle <list_resources/> element. This requires special handling due to the data types of some of the attributes.

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

Definition at line 1147 of file left_right.py.

13.125.2.2 def rpki.left_right.list_resources_elt.toXML (self)

Generate <list_resources/> element. This requires special handling due to the data types of some of the attributes.

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

Definition at line 1163 of file left_right.py.

13.125.3 Member Data Documentation

13.125.3.1 rpki.left_right.list_resources_elt.asn

Definition at line 1150 of file left_right.py.

```
13.125.3.2 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 1144 of file left_right.py.

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

Definition at line 1143 of file left_right.py.

13.125.3.4 rpki.left_right.list_resources_elt.ipv4

Definition at line 1150 of file left_right.py.

13.125.3.5 rpki.left_right.list_resources_elt.ipv6

Definition at line 1150 of file left_right.py.

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

Definition at line 1145 of file left_right.py.

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

- [left_right.py \(3793\)](#)

13.126 rpki.left_right.list_roa_requests_elt Class Reference

Inheritance diagram for rpki.left_right.list_roa_requests_elt:

Collaboration diagram for rpki.left_right.list_roa_requests_elt:

Public Member Functions

- def [startElement](#)

Public Attributes

- [ipv4](#)
- [ipv6](#)

Static Public Attributes

- tuple [attributes](#) = ("self_handle", "tag", "asn", "[ipv4](#)", "[ipv6](#)")
XML attributes for this element.
- string [element_name](#) = "list_roa_requests"

13.126.1 Detailed Description

<list_roa_requests/> element.

Definition at line 1173 of file left_right.py.

13.126.2 Member Function Documentation

13.126.2.1 `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 1181 of file left_right.py.

13.126.3 Member Data Documentation

13.126.3.1 `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 1179 of file left_right.py.

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

Definition at line 1178 of file left_right.py.

13.126.3.3 `rpki.left_right.list_roa_requests_elt.ipv4`

Definition at line 1184 of file left_right.py.

13.126.3.4 `rpki.left_right.list_roa_requests_elt.ipv6`

Definition at line 1184 of file left_right.py.

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

- [left_right.py \(3793\)](#)

13.127 rpki.left_right.msg Class Reference

Inheritance diagram for rpki.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.

13.127.1 Detailed Description

Left-right PDU.

Definition at line 1305 of file left_right.py.

13.127.2 Member Function Documentation

13.127.2.1 def rpki.left_right.msg.serve_top_level (self, gctx, cb)

Serve one msg PDU.

Definition at line 1323 of file left_right.py.

13.127.3 Member Data Documentation

13.127.3.1 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_ghostbuster_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 1316 of file `left_right.py`.

13.127.3.2 rpki::left_right.msg::version = 1 [static]

Protocol version.

Reimplemented from [rpki.xml_utils.msg](#).

Definition at line 1312 of file `left_right.py`.

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

- [left_right.py \(3793\)](#)

13.128 rpki.left_right.parent_elt Class Reference

Inheritance diagram for `rpki.left_right.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_reissue](#)
- def [serve_rekey](#)
- def [serve_revoke](#)
- def [serve_revoke_forgotten](#)

Static Public Attributes

- tuple [attributes](#)

XML attributes for this element.

- tuple `booleans` = ("rekey", "reissue", "revoke", "revoke_forgotten")

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

- `bpki_cms_cert` = None
- `bpki_cms_glue` = None
- string `element_name` = "parent"
- tuple `elements` = ("bpki_cms_cert", "bpki_cms_glue")

XML elements contained by this element.

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

13.128.1 Detailed Description

`<parent/> element.`

Definition at line 853 of file `left_right.py`.

13.128.2 Member Function Documentation

13.128.2.1 `def rpki.left_right.parent_elt.cas (self)`

Fetch all CA objects that link to this parent object.

Definition at line 885 of file `left_right.py`.

13.128.2.2 `def rpki.left_right.parent_elt.query_up_down (self, q_pdu, cb, eb)`

Client code for sending one up-down query PDU to this parent.

Definition at line 972 of file `left_right.py`.

13.128.2.3 `def rpki.left_right.parent_elt.repository (self)`

Fetch repository object to which this parent object links.

Definition at line 878 of file left_right.py.

13.128.2.4 `def rpki.left_right.parent_elt.serve_post_save_hook (self, q_pdu,
r_pdu, cb, eb)`

Extra server actions for parent_elt.

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

Definition at line 891 of file left_right.py.

13.128.2.5 `def rpki.left_right.parent_elt.serve_reissue (self, cb, eb)`

Handle a left-right reissue action for this parent.

Definition at line 924 of file left_right.py.

13.128.2.6 `def rpki.left_right.parent_elt.serve_rekey (self, cb, eb)`

Handle a left-right rekey action for this parent.

Definition at line 908 of file left_right.py.

13.128.2.7 `def rpki.left_right.parent_elt.serve_revoke (self, cb, eb)`

Handle a left-right revoke action for this parent.

Definition at line 916 of file left_right.py.

13.128.2.8 `def rpki.left_right.parent_elt.serve_revoke_forgotten (self, cb, eb)`

Handle a left-right revoke_forgotten action for this parent.

This is a bit fiddly: we have to compare the result of an up-down list query with what we have locally and identify the SKIs of any certificates that have gone missing. This should never happen in ordinary operation, but can arise if we have somehow lost a private key, in which case there is nothing more we can do with the issued cert, so we have to clear it. As this really is not supposed to happen, we don't clear it automatically, instead we require an explicit trigger.

Definition at line 932 of file left_right.py.

13.128.3 Member Data Documentation

13.128.3.1 `tuple rpki.left_right.parent_elt.attributes [static]`

Initial value:

```
( "action", "tag", "self_handle", "parent_handle", "bsc_handle", "repository_handle",
  "peer_contact_uri", "sia_base", "sender_name", "recipient_name" )
```

XML attributes for this element.

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

Definition at line 859 of file left_right.py.

13.128.3.2 `tuple rpki.left_right.parent_elt.booleans = ("rekey", "reissue", "revoke", "revoke_forgotten") [static]`

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

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

Definition at line 862 of file left_right.py.

13.128.3.3 `rpki.left_right.parent_elt.bpkc_cert = None [static]`

Definition at line 874 of file left_right.py.

13.128.3.4 rpki.left_right.parent_elt.bpki_cms_glue = None [static]

Definition at line 875 of file left_right.py.

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

Definition at line 858 of file left_right.py.

13.128.3.6 tuple rpki.left_right.parent_elt.elements = ("bpki_cms_cert", "bpki_cms_glue") [static]

XML elements contained by this element.

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

Definition at line 861 of file left_right.py.

13.128.3.7 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 872 of file left_right.py.

13.128.3.8 tuple rpki.left_right.parent_elt.sql_template [static]

Initial value:

```
rpki.sql.template("parent", "parent_id", "parent_handle",
                  "self_id", "bsc_id", "repository_id",
                  "peer_contact_uri", "sia_base",
                  "sender_name", "recipient_name",
                  ("bpki_cms_cert", rpki.x509.X509),
                  ("bpki_cms_glue", rpki.x509.X509),
                  ("last_cms_timestamp", rpki.sundial.datetime))
```

Definition at line 864 of file left_right.py.

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

- [left_right.py \(3793\)](#)

13.129 rpki.left_right.report_error_elt Class Reference

Inheritance diagram for rpki.left_right.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.

13.129.1 Detailed Description

<report_error/> element.

Definition at line 1282 of file left_right.py.

13.129.2 Member Function Documentation

- ##### 13.129.2.1
- ```
def rpki.left_right.report_error_elt.from_exception (cls, e,
self_handle = None, tag = None)
```

Generate a `<report_error/>` element from an exception.

Definition at line 1294 of file `left_right.py`.

### 13.129.3 Member Data Documentation

**13.129.3.1** tuple `rpki.left_right.report_error_elt.attributes = ("tag", "self_handle", "error_code")` `[static]`

XML attributes for this element.

Reimplemented from `rpki.xml_utils.base_elt`.

Definition at line 1288 of file `left_right.py`.

**13.129.3.2** string `rpki.left_right.report_error_elt.element_name = "report_error"` `[static]`

Definition at line 1287 of file `left_right.py`.

**13.129.3.3** `rpki.left_right.report_error_elt.error_code`

Definition at line 1296 of file `left_right.py`.

**13.129.3.4** `rpki.left_right.report_error_elt.error_text = None` `[static]`

Definition at line 1291 of file `left_right.py`.

**13.129.3.5** `rpki.left_right.report_error_elt.self_handle`

Definition at line 1296 of file `left_right.py`.

**13.129.3.6** `rpki.left_right.report_error_elt.tag`

Definition at line 1296 of file left\_right.py.

```
13.129.3.7 string rpki.left_right.report_error_elt.text_attribute = "error_text"
 [static]
```

Name of the class attribute that holds the text value.

Reimplemented from [rpki.xml\\_utils.text\\_elt](#).

Definition at line 1289 of file left\_right.py.

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

- [left\\_right.py \(3793\)](#)

## 13.130 rpki.left\_right.repository\_elt Class Reference

Inheritance diagram for `rpki.left_right.repository_elt`:

Collaboration diagram for `rpki.left_right.repository_elt`:

### Public Member Functions

- def [call\\_pubd](#)
- def [default\\_pubd\\_handler](#)
- def [parents](#)

### Static Public Attributes

- tuple [attributes](#) = ("action", "tag", "[self\\_handle](#)", "repository\_handle", "bsc\_handle", "peer\_contact\_uri")

*XML attributes for this element.*

- [bpki\\_cert](#) = None
- [bpki\\_glue](#) = None
- string [element\\_name](#) = "repository"
- tuple [elements](#) = ("bpki\_cert", "[bpki\\_glue](#)")

*XML elements contained by this element.*

- tuple [handles](#) = (("self", [self\\_elt](#)), ("bsc", [bsc\\_elt](#)))
- tuple [sql\\_template](#)

### 13.130.1 Detailed Description

<repository/> element.

Definition at line 761 of file left\_right.py.

### 13.130.2 Member Function Documentation

#### 13.130.2.1 def rpki.left\_right.repository\_elt.call\_pubd ( *self*, *callback*, *errback*, *q\_msg*, *handlers* = *None* )

Send a message to publication daemon and return the response.

As a convenience, attempting to send an empty message returns immediate success without sending anything.

Handlers is a dict of handler functions to process the response PDUs. If the tag value in the response PDU appears in the dict, the associated handler is called to process the PDU. If no tag matches, default\_pubd\_handler() is called. A handler value of False suppresses calling of the default handler.

Definition at line 795 of file left\_right.py.

#### 13.130.2.2 def rpki.left\_right.repository\_elt.default\_pubd\_handler ( *pdu* )

Default handler for publication response PDUs.

Definition at line 789 of file left\_right.py.

#### 13.130.2.3 def rpki.left\_right.repository\_elt.parents ( *self* )

Fetch all parent objects that link to this repository object.

Definition at line 782 of file left\_right.py.

### 13.130.3 Member Data Documentation

**13.130.3.1** `tuple rpki.left_right.repository_elt.attributes = ("action",  
"tag", "self_handle", "repository_handle", "bsc_handle",  
"peer_contact_uri") [static]`

XML attributes for this element.

Reimplemented from [rpki.xml\\_utils.base\\_elt](#).

Definition at line 767 of file left\_right.py.

**13.130.3.2** `rpki.left_right.repository_elt.bpki_cert = None [static]`

Definition at line 778 of file left\_right.py.

**13.130.3.3** `rpki.left_right.repository_elt.bpki_glue = None [static]`

Definition at line 779 of file left\_right.py.

**13.130.3.4** `string rpki.left_right.repository_elt.element_name = "repository"  
[static]`

Definition at line 766 of file left\_right.py.

**13.130.3.5** `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 768 of file left\_right.py.



### 13.130.3.6 tuple rpki.left\_right.repository\_elt.handles = (("self", self\_elt), ("bsc", bsc\_elt)) [static]

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

Definition at line 776 of file left\_right.py.

### 13.130.3.7 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", rpki.x509.X509),
 ("last_cms_timestamp", rpki.sundial.datetime))
```

Definition at line 770 of file left\_right.py.

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

- [left\\_right.py \(3793\)](#)

## 13.131 rpki.left\_right.sax\_handler Class Reference

Inheritance diagram for rpki.left\_right.sax\_handler:

Collaboration diagram for rpki.left\_right.sax\_handler:

### Static Public Attributes

- string [name](#) = "msg"
- [pdu](#) = [msg](#)
- string [version](#) = "1"

### 13.131.1 Detailed Description

SAX handler for Left-Right protocol.

Definition at line 1351 of file left\_right.py.

### 13.131.2 Member Data Documentation

#### 13.131.2.1 string rpki.left\_right.sax\_handler.name = "msg" [static]

Definition at line 1357 of file left\_right.py.

#### 13.131.2.2 rpki.left\_right.sax\_handler.pdu = msg [static]

Reimplemented in [irbe\\_cli.left\\_right\\_sax\\_handler](#).

Definition at line 1356 of file left\_right.py.

#### 13.131.2.3 string rpki.left\_right.sax\_handler.version = "1" [static]

Definition at line 1358 of file left\_right.py.

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

- [left\\_right.py](#) (3793)

### 13.132 rpki.left\_right.self\_elt Class Reference

Inheritance diagram for rpki.left\_right.self\_elt:

Collaboration diagram for rpki.left\_right.self\_elt:

#### Public Member Functions

- def [bscs](#)
- def [children](#)
- def [client\\_poll](#)
- def [cron](#)
- def [ghostbusters](#)
- 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\\_reissue](#)
- def [serve\\_rekey](#)
- def [serve\\_revoke](#)
- def [serve\\_revoke\\_forgotten](#)
- def [serve\\_run\\_now](#)
- def [update\\_children](#)
- def [update\\_ghostbusters](#)
- def [update\\_roas](#)

#### Static Public Attributes

- tuple [attributes](#) = ("action", "tag", "[self\\_handle](#)", "[crl\\_interval](#)", "[regen\\_margin](#)")

*XML attributes for this element.*

- tuple [booleans](#) = ("rekey", "reissue", "revoke", "run\_now", "publish\_world\_now", "revoke\_forgotten")

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

- [bpki\\_cert](#) = None
- [bpki\\_glue](#) = None
- [crl\\_interval](#) = None
- string [element\\_name](#) = "self"
- tuple [elements](#) = ("[bpki\\_cert](#)", "[bpki\\_glue](#)")

*XML elements contained by this element.*

- tuple [handles](#) = ()
- [regen\\_margin](#) = None
- tuple [sql\\_template](#)
- [use\\_hsm](#) = False

#### 13.132.1 Detailed Description

<self/> element.

Definition at line 130 of file left\_right.py.

### 13.132.2 Member Function Documentation

#### 13.132.2.1 def rpki.left\_right.self\_elt.bscs ( *self* )

Fetch all BSC objects that link to this self object.

Definition at line 152 of file left\_right.py.

#### 13.132.2.2 def rpki.left\_right.self\_elt.children ( *self* )

Fetch all child objects that link to this self object.

Definition at line 173 of file left\_right.py.

#### 13.132.2.3 def rpki.left\_right.self\_elt.client\_poll ( *self*, *callback* )

Run the regular client poll cycle with each of this self's parents in turn.

Definition at line 346 of file left\_right.py.

#### 13.132.2.4 def rpki.left\_right.self\_elt.cron ( *self*, *cb* )

Periodic tasks.

Definition at line 313 of file left\_right.py.

#### 13.132.2.5 def rpki.left\_right.self\_elt.ghostbusters ( *self* )

Fetch all Ghostbuster record objects that link to this self object.

Definition at line 187 of file left\_right.py.

**13.132.2.6 def rpki.left\_right.self\_elt.parents ( *self* )**

Fetch all parent objects that link to this self object.

Definition at line 166 of file left\_right.py.

**13.132.2.7 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 484 of file left\_right.py.

**13.132.2.8 def rpki.left\_right.self\_elt.repositories ( *self* )**

Fetch all repository objects that link to this self object.

Definition at line 159 of file left\_right.py.

**13.132.2.9 def rpki.left\_right.self\_elt.roas ( *self* )**

Fetch all ROA objects that link to this self object.

Definition at line 180 of file left\_right.py.

**13.132.2.10 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 305 of file left\_right.py.

**13.132.2.11** `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 299 of file left\_right.py.

**13.132.2.12** `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 291 of file left\_right.py.

**13.132.2.13** `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 193 of file left\_right.py.

**13.132.2.14** `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 251 of file left\_right.py.

#### 13.132.2.15 def rpki.left\_right.self\_elt.serve\_reissue ( self, cb, eb )

Handle a left-right reissue action for this self.

Definition at line 233 of file left\_right.py.

#### 13.132.2.16 def rpki.left\_right.self\_elt.serve\_rekey ( self, cb, eb )

Handle a left-right rekey action for this self.

Definition at line 215 of file left\_right.py.

#### 13.132.2.17 def rpki.left\_right.self\_elt.serve\_revoke ( self, cb, eb )

Handle a left-right revoke action for this self.

Definition at line 224 of file left\_right.py.

#### 13.132.2.18 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 242 of file left\_right.py.

**13.132.2.19** `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 284 of file left\_right.py.

**13.132.2.20** `def rpki.left_right.self_elt.update_children ( self, cb )`

Check for updated IRDB data for all of this self's children and issue new certs as necessary. Must handle changes both in resources and in expiration date.

Definition at line 405 of file left\_right.py.

**13.132.2.21** `def rpki.left_right.self_elt.update_ghostbusters ( self, cb )`

Generate or update Ghostbuster records for this self.

This is heavily based on .update\_roas(), and probably both of them need refactoring.

Definition at line 528 of file left\_right.py.

**13.132.2.22** `def rpki.left_right.self_elt.update_roas ( self, cb )`

Generate or update ROAs for this self.

Definition at line 618 of file left\_right.py.

**13.132.3** Member Data Documentation**13.132.3.1** `tuple rpki.left_right.self_elt.attributes = ("action", "tag", "self_handle", "crl_interval", "regen_margin") [static]`

XML attributes for this element.

Reimplemented from [rpki.xml\\_utils.base\\_elt](#).

Definition at line 136 of file left\_right.py.



**13.132.3.2** `tuple rpki.left_right.self_elt.booleans = ("rekey", "reissue",  
"revoke", "run_now", "publish_world_now", "revoke_forgotten")  
[static]`

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

Reimplemented from [rpki.xml\\_utils.base\\_elt](#).

Definition at line 138 of file left\_right.py.

**13.132.3.3** `rpki.left_right.self_elt.bpki_cert = None [static]`

Definition at line 148 of file left\_right.py.

**13.132.3.4** `rpki.left_right.self_elt.bpki_glue = None [static]`

Definition at line 149 of file left\_right.py.

**13.132.3.5** `rpki.left_right.self_elt.crl_interval = None [static]`

Definition at line 146 of file left\_right.py.

**13.132.3.6** `string rpki.left_right.self_elt.element_name = "self" [static]`

Definition at line 135 of file left\_right.py.

**13.132.3.7** `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 137 of file left\_right.py.

**13.132.3.8 tuple rpki.left\_right.self\_elt.handles = () [static]**

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

Definition at line 143 of file left\_right.py.

**13.132.3.9 rpki.left\_right.self\_elt.regen\_margin = None [static]**

Definition at line 147 of file left\_right.py.

**13.132.3.10 tuple rpki.left\_right.self\_elt.sql\_template [static]**

**Initial value:**

```
rpki.sql.template("self", "self_id", "self_handle",
 "use_hsm", "crl_interval", "regen_margin",
 ("bpki_cert", rpki.x509.X509), ("bpki_glue", r
pki.x509.X509))
```

Definition at line 140 of file left\_right.py.

**13.132.3.11 rpki.left\_right.self\_elt.use\_hsm = False [static]**

Definition at line 145 of file left\_right.py.

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

- [left\\_right.py \(3793\)](#)

**13.133 rpki.log.logger Class Reference**

Inheritance diagram for rpki.log.logger:

Collaboration diagram for rpki.log.logger:

**Public Member Functions**

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

### Public Attributes

- [priority](#)

#### 13.133.1 Detailed Description

Closure for logging.

Definition at line 76 of file log.py.

#### 13.133.2 Constructor & Destructor Documentation

##### 13.133.2.1 def rpki.log.logger.\_\_init\_\_ ( *self*, *priority* )

Definition at line 81 of file log.py.

#### 13.133.3 Member Function Documentation

##### 13.133.3.1 def rpki.log.logger.\_\_call\_\_ ( *self*, *message* )

Definition at line 84 of file log.py.

#### 13.133.4 Member Data Documentation

##### 13.133.4.1 rpki.log.logger.priority

Definition at line 81 of file log.py.

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

- [log.py \(3793\)](#)

### 13.134 rpki.manifest.FileAndHash Class Reference

Inheritance diagram for rpki.manifest.FileAndHash:

Collaboration diagram for rpki.manifest.FileAndHash:

### Public Member Functions

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

### Public Attributes

- [file](#)
- [hash](#)

#### 13.134.1 Detailed Description

Definition at line 27 of file manifest.py.

#### 13.134.2 Constructor & Destructor Documentation

**13.134.2.1** `def rpki.manifest.FileAndHash.__init__( self, optional = 0, default = " )`

Definition at line 28 of file manifest.py.

#### 13.134.3 Member Data Documentation

##### 13.134.3.1 rpki.manifest.FileAndHash.file

Definition at line 28 of file manifest.py.

##### 13.134.3.2 rpki.manifest.FileAndHash.hash

Definition at line 28 of file manifest.py.

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

- [manifest.py \(3598\)](#)

### 13.135 rpki.manifest.FilesAndHashes Class Reference

Inheritance diagram for rpki.manifest.FilesAndHashes:

Collaboration diagram for rpki.manifest.FilesAndHashes:

**Public Member Functions**

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

**13.135.1 Detailed Description**

Definition at line 34 of file manifest.py.

**13.135.2 Constructor & Destructor Documentation****13.135.2.1** `def rpki.manifest.FilesAndHashes.__init__( self, optional = 0, default = " ")`

Definition at line 35 of file manifest.py.

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

- [manifest.py \(3598\)](#)

**13.136 rpki.manifest.Manifest Class Reference**

Inheritance diagram for rpki.manifest.Manifest:

Collaboration diagram for rpki.manifest.Manifest:

**Public Member Functions**

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

**Public Attributes**

- [explicitVersion](#)
- [fileHashAlg](#)
- [fileList](#)
- [manifestNumber](#)
- [nextUpdate](#)
- [thisUpdate](#)
- [version](#)

**13.136.1 Detailed Description**

Definition at line 38 of file manifest.py.

### 13.136.2 Constructor & Destructor Documentation

**13.136.2.1** `def rpki.manifest.Manifest.__init__( self, optional = 0, default =  
" )`

Definition at line 39 of file manifest.py.

### 13.136.3 Member Data Documentation

**13.136.3.1** `rpki.manifest.Manifest.explicitVersion`

Definition at line 39 of file manifest.py.

**13.136.3.2** `rpki.manifest.Manifest.fileHashAlg`

Definition at line 39 of file manifest.py.

**13.136.3.3** `rpki.manifest.Manifest.fileList`

Definition at line 39 of file manifest.py.

**13.136.3.4** `rpki.manifest.Manifest.manifestNumber`

Definition at line 39 of file manifest.py.

**13.136.3.5** `rpki.manifest.Manifest.nextUpdate`

Definition at line 39 of file manifest.py.

**13.136.3.6** `rpki.manifest.Manifest.thisUpdate`

Definition at line 39 of file manifest.py.

### 13.136.3.7 rpki.manifest.Manifest.version

Definition at line 39 of file manifest.py.

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

- [manifest.py \(3598\)](#)

## 13.137 rpki.myrpki.CA Class Reference

Inheritance diagram for rpki.myrpki.CA:

Collaboration diagram for rpki.myrpki.CA:

### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [bsc](#)
- def [cms\\_xml\\_sign](#)
- def [cms\\_xml\\_verify](#)
- def [ee](#)
- def [fxcert](#)
- def [run\\_ca](#)
- def [run\\_dgst](#)
- def [run\\_openssl](#)
- def [run\\_req](#)
- def [setup](#)
- def [touch\\_file](#)
- def [xcert](#)
- def [xcert\\_filename](#)
- def [xcert\\_revoke](#)

### Public Attributes

- [cer](#)
- [cfg](#)
- [crl](#)
- [crlnum](#)
- [dir](#)

- [env](#)
- [index](#)
- [key](#)
- [openssl](#)
- [req](#)
- [serial](#)

#### Static Public Attributes

- dictionary [path\\_restriction](#)

#### 13.137.1 Detailed Description

Representation of one certification authority.

Definition at line 573 of file myrpki.py.

#### 13.137.2 Constructor & Destructor Documentation

##### 13.137.2.1 `def rpki.myrpki.CA.__init__( self, cfg_file, dir )`

Definition at line 584 of file myrpki.py.

#### 13.137.3 Member Function Documentation

##### 13.137.3.1 `def rpki.myrpki.CA.bsc( self, pkcs10 )`

Issue BSC certificate, if we have a PKCS #10 request for it.

Definition at line 737 of file myrpki.py.

##### 13.137.3.2 `def rpki.myrpki.CA.cms_xml_sign( self, ee_name, base_name, elt )`

Sign an XML object with CMS, return Base64 text.

Definition at line 699 of file myrpki.py.



**13.137.3.3 def rpki.myrpki.CA.cms\_xml\_verify ( self, b64, ca )**

Attempt to verify and extract XML from a Base64-encoded signed CMS object. CA is the filename of a certificate that we expect to be the issuer of the EE certificate bundled with the CMS, and must previously have been cross-certified under our trust anchor.

Definition at line 712 of file myrpki.py.

**13.137.3.4 def rpki.myrpki.CA.aa ( self, ee\_name, base\_name )**

Issue an end-entity certificate.

Definition at line 685 of file myrpki.py.

**13.137.3.5 def rpki.myrpki.CA.fxcert ( self, b64, filename = None, path\_restriction = 0 )**

Write PEM certificate to file, then cross-certify.

Definition at line 758 of file myrpki.py.

**13.137.3.6 def rpki.myrpki.CA.run\_ca ( self, args )**

Run OpenSSL "ca" command with common initial arguments.

Definition at line 619 of file myrpki.py.

**13.137.3.7 def rpki.myrpki.CA.run\_dgst ( self, input, algorithm = "md5" )**

Run OpenSSL "dgst" command, return cleaned-up result.

Definition at line 636 of file myrpki.py.

**13.137.3.8** `def rpki.myrpki.CA.run_openssl ( self, cmd, kwargs )`

Run an OpenSSL command, suppresses stderr unless OpenSSL returns failure, and returns stdout.

Definition at line 603 of file myrpki.py.

**13.137.3.9** `def rpki.myrpki.CA.run_req ( self, key_file, req_file, log_key = sys.stdout )`

Run OpenSSL "genrsa" and "req" commands.

Definition at line 625 of file myrpki.py.

**13.137.3.10** `def rpki.myrpki.CA.setup ( self, ca_name )`

Set up this CA. ca\_name is an X.509 distinguished name in /tag=val/tag=val format.

Definition at line 659 of file myrpki.py.

**13.137.3.11** `def rpki.myrpki.CA.touch_file ( filename, content = None )`

Create dumb little text files expected by OpenSSL "ca" utility.

Definition at line 649 of file myrpki.py.

**13.137.3.12** `def rpki.myrpki.CA.xcert ( self, cert, path_restriction = 0 )`

Cross-certify a certificate represented as a PEM file, if we haven't already. This only works for self-signed certs, due to limitations of the OpenSSL command line tool, but that suffices for our purposes.

Definition at line 785 of file myrpki.py.

**13.137.3.13 def rpki.myrpki.CA.xcert\_filename ( *self*, *cert* )**

Generate filename for a cross-certification.

Extracts public key and subject name from PEM file and hash it so we can use the result as a tag for cross-certifying this cert.

Definition at line 771 of file myrpki.py.

**13.137.3.14 def rpki.myrpki.CA.xcert\_revoke ( *self*, *cert* )**

Revoke a cross-certification and regenerate CRL.

Definition at line 798 of file myrpki.py.

**13.137.4 Member Data Documentation****13.137.4.1 rpki.myrpki.CA.cer**

Definition at line 584 of file myrpki.py.

**13.137.4.2 rpki.myrpki.CA.cfg**

Definition at line 584 of file myrpki.py.

**13.137.4.3 rpki.myrpki.CA.crl**

Definition at line 584 of file myrpki.py.

**13.137.4.4 rpki.myrpki.CA.crlnum**

Definition at line 584 of file myrpki.py.

#### 13.137.4.5 rpki.myrpki.CA.dir

Definition at line 584 of file myrpki.py.

#### 13.137.4.6 rpki.myrpki.CA.env

Definition at line 584 of file myrpki.py.

#### 13.137.4.7 rpki.myrpki.CA.index

Definition at line 584 of file myrpki.py.

#### 13.137.4.8 rpki.myrpki.CA.key

Definition at line 584 of file myrpki.py.

#### 13.137.4.9 rpki.myrpki.CA.openssl

Definition at line 584 of file myrpki.py.

#### 13.137.4.10 dictionary rpki.myrpki.CA.path\_restriction [static]

**Initial value:**

```
{ 0 : "ca_x509_ext_xcert0",
 1 : "ca_x509_ext_xcert1" }
```

Definition at line 581 of file myrpki.py.

#### 13.137.4.11 rpki.myrpki.CA.req

Definition at line 584 of file myrpki.py.

### 13.137.4.12 rpki.myrpki.CA.serial

Definition at line 584 of file myrpki.py.

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

- [myrpki.py \(3793\)](#)

## 13.138 rpki.myrpki.child Class Reference

Inheritance diagram for rpki.myrpki.child:

Collaboration diagram for rpki.myrpki.child:

### Public Member Functions

- [def \\_\\_init\\_\\_](#)
- [def \\_\\_repr\\_\\_](#)
- [def add](#)
- [def xml](#)

### Public Attributes

- [asns](#)
- [bpki\\_certificate](#)
- [handle](#)
- [v4](#)
- [v6](#)
- [validity](#)

### Static Public Attributes

- `tuple v4re = re.compile("^(([0-9]{1,3}\.){3}[0-9]{1,3}/[0-9]+)|((([0-9]{1,3}\.){3}[0-9]{1,3})-([0-9]{1,3}\.){3}[0-9]{1,3})$", re.I)`
- `tuple v6re = re.compile("^(([0-9a-f]{0,4}:){0,15}[0-9a-f]{0,4}/[0-9]+)|((([0-9a-f]{0,4}:){0,15}[0-9a-f]{0,4})-([0-9a-f]{0,4}:){0,15}[0-9a-f]{0,4})$", re.I)`

### 13.138.1 Detailed Description

Representation of one child entity.

Definition at line 187 of file myrpki.py.

### 13.138.2 Constructor & Destructor Documentation

#### 13.138.2.1 def rpki.myrpki.child.\_\_init\_\_( self, handle )

Definition at line 195 of file myrpki.py.

### 13.138.3 Member Function Documentation

#### 13.138.3.1 def rpki.myrpki.child.\_\_repr\_\_( self )

Definition at line 203 of file myrpki.py.

#### 13.138.3.2 def rpki.myrpki.child.add ( self, prefix = None, asn = None, validity = None, bpki\_certificate = None )

Add prefix, autonomous system number, validity date, or BPKI certificate for this child.

Definition at line 217 of file myrpki.py.

#### 13.138.3.3 def rpki.myrpki.child.xml ( self, e )

Render this child as an XML element.

Definition at line 236 of file myrpki.py.

### 13.138.4 Member Data Documentation

#### 13.138.4.1 rpki.myrpki.child.asns

Definition at line 195 of file myrpki.py.

**13.138.4.2 rpki.myrpki.child.bpk\_certificate**

Definition at line 195 of file myrpki.py.

**13.138.4.3 rpki.myrpki.child.handle**

Definition at line 195 of file myrpki.py.

**13.138.4.4 rpki.myrpki.child.v4**

Definition at line 195 of file myrpki.py.

```
13.138.4.5 tuple rpki.myrpki.child.v4re = re.compile("^(([0-9]{1,3}\.){3}[0-9]{1,3}/[0-9]+)|((([0-9]{1,3}\.){3}[0-9]{1,3}-([0-9]{1,3}\.){3}[0-9]{1,3}))$", re.I) [static]
```

Definition at line 192 of file myrpki.py.

**13.138.4.6 rpki.myrpki.child.v6**

Definition at line 195 of file myrpki.py.

```
13.138.4.7 tuple rpki.myrpki.child.v6re = re.compile("^((([0-9a-f]{0,4}):(0,15)[0-9a-f]{0,4}/[0-9]+)|((([0-9a-f]{0,4}):(0,15)[0-9a-f]{0,4}-([0-9a-f]{0,4}):(0,15)[0-9a-f]{0,4}))$", re.I) [static]
```

Definition at line 193 of file myrpki.py.

**13.138.4.8 rpki.myrpki.child.validity**

Definition at line 195 of file myrpki.py.

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

- [myrpki.py \(3793\)](#)

## 13.139 rpki.myrpki.children Class Reference

Inheritance diagram for rpki.myrpki.children:

Collaboration diagram for rpki.myrpki.children:

### Public Member Functions

- def [add](#)
- def [from\\_entitydb](#)
- def [xml](#)

#### 13.139.1 Detailed Description

Database of children.

Definition at line 254 of file myrpki.py.

#### 13.139.2 Member Function Documentation

**13.139.2.1** `def rpki.myrpki.children.add ( self, handle, prefix = None, asn = None, validity = None, bpki_certificate = None )`

Add resources to a child, creating the child object if necessary.

Definition at line 259 of file myrpki.py.

**13.139.2.2** `def rpki.myrpki.children.from_entitydb ( cls, prefix_csv_file, asn_csv_file, fxcert, entitydb )`

Parse child data from entitydb.

Definition at line 275 of file myrpki.py.



### 13.139.2.3 def rpki.myrpki.children.xml ( self, e )

Render children database to XML.

Definition at line 267 of file myrpki.py.

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

- [myrpki.py \(3793\)](#)

## 13.140 rpki.myrpki.comma\_set Class Reference

Inheritance diagram for rpki.myrpki.comma\_set:

Collaboration diagram for rpki.myrpki.comma\_set:

### Public Member Functions

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

#### 13.140.1 Detailed Description

Minor customization of set(), to provide a print syntax.

Definition at line 86 of file myrpki.py.

#### 13.140.2 Member Function Documentation

##### 13.140.2.1 def rpki.myrpki.comma\_set.\_\_str\_\_ ( self )

Definition at line 91 of file myrpki.py.

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

- [myrpki.py \(3793\)](#)

## 13.141 rpki.myrpki.csv\_reader Class Reference

Inheritance diagram for rpki.myrpki.csv\_reader:

Collaboration diagram for rpki.myrpki.csv\_reader:

### Public Member Functions

- [def \\_\\_init\\_\\_](#)
- [def \\_\\_iter\\_\\_](#)

### Public Attributes

- [columns](#)
- [comment\\_characters](#)
- [file](#)
- [filename](#)
- [min\\_columns](#)

#### 13.141.1 Detailed Description

Reader for tab-delimited text that's (slightly) friendlier than the stock Python csv module (which isn't intended for direct use by humans anyway, and neither was this package originally, but that seems to be the way that it has evolved...).

Columns parameter specifies how many columns users of the reader expect to see; lines with fewer columns will be padded with None values.

Original API design for this class courtesy of Warren Kumari, but don't blame him if you don't like what I did with his ideas.

Definition at line 475 of file myrpki.py.

#### 13.141.2 Constructor & Destructor Documentation

**13.141.2.1** `def rpki.myrpki.csv_reader.__init__( self, filename, columns = None, min_columns = None, comment_characters = "#; " )`

Definition at line 490 of file myrpki.py.

#### 13.141.3 Member Function Documentation

**13.141.3.1** `def rpki.myrpki.csv_reader.__iter__( self )`

Definition at line 501 of file myrpki.py.

#### 13.141.4 Member Data Documentation

##### 13.141.4.1 rpki.myrpki.csv\_reader.columns

Definition at line 490 of file myrpki.py.

##### 13.141.4.2 rpki.myrpki.csv\_reader.comment\_characters

Definition at line 490 of file myrpki.py.

##### 13.141.4.3 rpki.myrpki.csv\_reader.file

Definition at line 490 of file myrpki.py.

##### 13.141.4.4 rpki.myrpki.csv\_reader.filename

Definition at line 490 of file myrpki.py.

##### 13.141.4.5 rpki.myrpki.csv\_reader.min\_columns

Definition at line 490 of file myrpki.py.

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

- [myrpki.py \(3793\)](#)

#### 13.142 rpki.myrpki.csv\_writer Class Reference

Inheritance diagram for rpki.myrpki.csv\_writer:

Collaboration diagram for rpki.myrpki.csv\_writer:

##### Public Member Functions

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

- def [\\_\\_init\\_\\_](#)
- def [close](#)

#### Public Attributes

- [file](#)
- [filename](#)
- [renmwo](#)
- [writer](#)

#### 13.142.1 Detailed Description

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

If "renmwo" is set (default), the file will be written to a temporary name and renamed to the real filename after closing.

Definition at line 517 of file myrpki.py.

#### 13.142.2 Constructor & Destructor Documentation

##### 13.142.2.1 def rpki.myrpki.csv\_writer.\_\_init\_\_( self, filename, renmwo = True )

Definition at line 526 of file myrpki.py.

#### 13.142.3 Member Function Documentation

##### 13.142.3.1 def rpki.myrpki.csv\_writer.\_\_getattr\_\_( self, attr )

Fake inheritance from whatever object csv.writer deigns to give us.

Definition at line 542 of file myrpki.py.

##### 13.142.3.2 def rpki.myrpki.csv\_writer.close( self )

Close this writer.

Definition at line 532 of file myrpki.py.

#### 13.142.4 Member Data Documentation

##### 13.142.4.1 rpki.myrpki.csv\_writer.file

Definition at line 526 of file myrpki.py.

##### 13.142.4.2 rpki.myrpki.csv\_writer.filename

Definition at line 526 of file myrpki.py.

##### 13.142.4.3 rpki.myrpki.csv\_writer.renmwo

Definition at line 526 of file myrpki.py.

##### 13.142.4.4 rpki.myrpki.csv\_writer.writer

Definition at line 526 of file myrpki.py.

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

- [myrpki.py \(3793\)](#)

#### 13.143 rpki.myrpki.EntityDB Class Reference

Inheritance diagram for rpki.myrpki.EntityDB:

Collaboration diagram for rpki.myrpki.EntityDB:

##### Public Member Functions

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

### Public Attributes

- [dir](#)
- [identity](#)

#### 13.143.1 Detailed Description

Wrapper for entitydb path lookups and iterations.

Definition at line 94 of file myrpki.py.

#### 13.143.2 Constructor & Destructor Documentation

##### 13.143.2.1 `def rpki.myrpki.EntityDB.__init__( self, cfg )`

Definition at line 99 of file myrpki.py.

#### 13.143.3 Member Function Documentation

##### 13.143.3.1 `def rpki.myrpki.EntityDB.__call__( self, dirname, filebase = None )`

Definition at line 103 of file myrpki.py.

##### 13.143.3.2 `def rpki.myrpki.EntityDB.iterate( self, dir, base = "*" )`

Definition at line 109 of file myrpki.py.

#### 13.143.4 Member Data Documentation

##### 13.143.4.1 `rpki.myrpki.EntityDB.dir`

Definition at line 99 of file myrpki.py.

### 13.143.4.2 rpki.myrpki.EntityDB.identity

Definition at line 99 of file myrpki.py.

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

- [myrpki.py \(3793\)](#)

## 13.144 rpki.myrpki.IRDB Class Reference

Inheritance diagram for rpki.myrpki.IRDB:

Collaboration diagram for rpki.myrpki.IRDB:

### Public Member Functions

- [def \\_\\_init\\_\\_](#)
- [def close](#)
- [def update](#)

### Public Attributes

- [db](#)

#### 13.144.1 Detailed Description

Front-end to the IRDB. This is broken out from class main so that other applications (namely, the portal-gui) can reuse it.

Definition at line 891 of file myrpki.py.

#### 13.144.2 Constructor & Destructor Documentation

##### 13.144.2.1 def rpki.myrpki.IRDB.\_\_init\_\_( self, cfg )

Opens a new connection to the IRDB, using the configuration information from a `rpki.config.parser` object.

Definition at line 896 of file myrpki.py.

### 13.144.3 Member Function Documentation

#### 13.144.3.1 def rpki.myrpki.IRDB.close ( *self* )

Close the connection to the IRDB.

Definition at line 1000 of file myrpki.py.

#### 13.144.3.2 def rpki.myrpki.IRDB.update ( *self*, *handle*, *roa\_requests*, *children*, *ghostbusters* = *None* )

Update the IRDB for a given resource handle. Removes all existing data and replaces it with that specified in the argument list.

The "roa\_requests" argument is a sequence of tuples of the form (asID, v4\_addresses, v6\_addresses), where "v\*\_addresses" are instances of rpki.resource\_set.roa\_prefix\_set\_ipv\*.

The "children" argument is a sequence of tuples of the form (child\_handle, asns, v4addrs, v6addrs, valid\_until), where "asns" is an instance of rpki.resource\_set.resource\_set\_asn, "v\*addrs" are instances of rpki.resource\_set.resource\_set\_ipv\*, and "valid\_until" is an instance of rpki.sundial.datetime.

The "ghostbusters" argument is a sequence of tuples of the form (parent\_handle, vcard\_string). "parent\_handle" may be value None, in which case the specified vcard object will be used for all parents.

Definition at line 915 of file myrpki.py.

### 13.144.4 Member Data Documentation

#### 13.144.4.1 rpki.myrpki.IRDB.db

Definition at line 899 of file myrpki.py.

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

- [myrpki.py \(3793\)](#)



### 13.145 rpki.myrpki.main Class Reference

Inheritance diagram for rpki.myrpki.main:

Collaboration diagram for rpki.myrpki.main:

#### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [complete\\_delete\\_child](#)
- def [complete\\_delete\\_parent](#)
- def [complete\\_delete\\_publication\\_client](#)
- def [complete\\_delete\\_repository](#)
- def [complete\\_renew\\_child](#)
- def [configure\\_resources\\_main](#)
- def [do\\_configure\\_child](#)
- def [do\\_configure\\_daemons](#)
- def [do\\_configure\\_parent](#)
- def [do\\_configure\\_publication\\_client](#)
- def [do\\_configure\\_repository](#)
- def [do\\_configure\\_resources](#)
- def [do\\_delete\\_child](#)
- def [do\\_delete\\_parent](#)
- def [do\\_delete\\_publication\\_client](#)
- def [do\\_delete\\_repository](#)
- def [do\\_initialize](#)
- def [do\\_renew\\_all\\_children](#)
- def [do\\_renew\\_child](#)
- def [do\\_update\\_bpki](#)
- def [entitydb\\_complete](#)
- def [help\\_overview](#)
- def [read\\_config](#)
- def [renew\\_children\\_common](#)

#### Public Attributes

- [bpki\\_resources](#)
- [bpki\\_servers](#)
- [cfg](#)
- [cfg\\_file](#)
- [default\\_repository](#)
- [entitydb](#)
- [handle](#)

- [histfile](#)
- [pubd\\_contact\\_info](#)
- [rsync\\_module](#)
- [rsync\\_server](#)
- [run\\_pubd](#)
- [run\\_rootd](#)
- [run\\_rpkid](#)

#### Static Public Attributes

- [completedefault](#) = rpki.cli.Cmd.filename\_complete
- string [prompt](#) = "myrpki> "
- [show\\_xml](#) = False

#### 13.145.1 Detailed Description

Definition at line 1008 of file myrpki.py.

#### 13.145.2 Constructor & Destructor Documentation

##### 13.145.2.1 `def rpki.myrpki.main.__init__( self )`

Definition at line 1016 of file myrpki.py.

#### 13.145.3 Member Function Documentation

##### 13.145.3.1 `def rpki.myrpki.main.complete_delete_child( self, args )`

Definition at line 1303 of file myrpki.py.

##### 13.145.3.2 `def rpki.myrpki.main.complete_delete_parent( self, args )`

Definition at line 1366 of file myrpki.py.

**13.145.3.3** `def rpki.myrpki.main.complete_delete_publication_client ( self, args )`

Definition at line 1469 of file myrpki.py.

**13.145.3.4** `def rpki.myrpki.main.complete_delete_repository ( self, args )`

Definition at line 1517 of file myrpki.py.

**13.145.3.5** `def rpki.myrpki.main.complete_renew_child ( self, args )`

Definition at line 1562 of file myrpki.py.

**13.145.3.6** `def rpki.myrpki.main.configure_resources_main ( self, msg = None )`

Main program of old myrpki.py script. This remains separate because it's called from more than one place.

Definition at line 1574 of file myrpki.py.

**13.145.3.7** `def rpki.myrpki.main.do_configure_child ( self, arg )`

Configure a new child of this RPKI entity, given the child's XML identity file as an input. This command extracts the child's data from the XML, cross-certifies the child's resource-holding BPKI certificate, and generates an XML file describing the relationship between the child and this parent, including this parent's BPKI data and up-down protocol service URI.

Definition at line 1207 of file myrpki.py.

**13.145.3.8** `def rpki.myrpki.main.do_configure_daemons ( self, arg )`

Configure RPKI daemons with the data built up by the other commands in this program.

The basic model here is that each entity with resources to certify runs the myrpki tool, but not all of them necessarily run their own RPKI engines. The entities that do run RPKI engines get data from the entities they host via the XML files output by the `configure_resources` command. Those XML files are the input to this command, which uses them to do all the work of configuring daemons, populating SQL databases, and so forth. A few operations (eg, BSC construction) generate data which has to be shipped back to the resource holder, which we do by updating the same XML file.

In essence, the XML files are a sneakernet (or email, or carrier pigeon) communication channel between the resource holders and the RPKI engine operators.

As a convenience, for the normal case where the RPKI engine operator is itself a resource holder, this command in effect runs the `configure_resources` command automatically to process the RPKI engine operator's own resources.

Note that, due to the back and forth nature of some of these operations, it may take several cycles for data structures to stabilize and everything to reach a steady state. This is normal.

Definition at line 1642 of file `myrpki.py`.

#### 13.145.3.9 `def rpki.myrpki.main.do_configure_parent ( self, arg )`

Configure a new parent of this RPKI entity, given the output of the parent's `configure_child` command as input. This command reads the parent's response XML, extracts the parent's BPKI and service URI information, cross-certifies the parent's BPKI data into this entity's BPKI, and checks for offers or referrals of publication service. If a publication offer or referral is present, we generate a request-for-service message to that repository, in case the user wants to avail herself of the referral or offer.

Definition at line 1307 of file `myrpki.py`.

#### 13.145.3.10 `def rpki.myrpki.main.do_configure_publication_client ( self, arg )`

Configure publication server to know about a new client, given the client's request-for-service message as input. This command reads the client's request for service, cross-certifies the client's BPKI data, and generates a response message containing the repository's BPKI data and service URI.

Definition at line 1370 of file myrpki.py.

#### 13.145.3.11 `def rpki.myrpki.main.do_configure_repository ( self, arg )`

Configure a publication repository for this RPKI entity, given the repository's response to our request-for-service message as input. This command reads the repository's response, extracts and cross-certifies the BPKI data and service URI, and links the repository data with the corresponding parent data in our local database.

Definition at line 1473 of file myrpki.py.

#### 13.145.3.12 `def rpki.myrpki.main.do_configure_resources ( self, arg )`

Read CSV files and all the descriptions of parents and children that we've built up, package the result up as a single XML file to be shipped to a hosting rpkiid.

Definition at line 1629 of file myrpki.py.

#### 13.145.3.13 `def rpki.myrpki.main.do_delete_child ( self, arg )`

Delete a child of this RPKI entity.

This should check that the XML file it's deleting really is a child, but doesn't, yet.

Definition at line 1290 of file myrpki.py.

#### 13.145.3.14 `def rpki.myrpki.main.do_delete_parent ( self, arg )`

Delete a parent of this RPKI entity.

This should check that the XML file it's deleting really is a parent, but doesn't, yet.

Definition at line 1353 of file myrpki.py.

**13.145.3.15 def rpki.myrpki.main.do\_delete\_publication\_client ( self, arg )**

Delete a publication client of this RPKI entity.

This should check that the XML file it's deleting really is a client, but doesn't, yet.

Definition at line 1456 of file myrpki.py.

**13.145.3.16 def rpki.myrpki.main.do\_delete\_repository ( self, arg )**

Delete a repository of this RPKI entity.

This should check that the XML file it's deleting really is a repository, but doesn't, yet.

Definition at line 1504 of file myrpki.py.

**13.145.3.17 def rpki.myrpki.main.do\_initialize ( self, arg )**

Initialize an RPKI installation. This command reads the configuration file, creates the BPKI and EntityDB directories, generates the initial BPKI certificates, and creates an XML file describing the resource-holding aspect of this RPKI installation.

Definition at line 1084 of file myrpki.py.

**13.145.3.18 def rpki.myrpki.main.do\_renew\_all\_children ( self, arg )**

Update validity period for all child entities.

Definition at line 1565 of file myrpki.py.

**13.145.3.19 def rpki.myrpki.main.do\_renew\_child ( self, arg )**

Update validity period for one child entity.

Definition at line 1556 of file myrpki.py.

**13.145.3.20 def rpki.myrpki.main.do\_update\_bpki ( *self*, *arg* )**

Update BPKI certificates. Assumes an existing RPKI installation.

Basic plan here is to reissue all BPKI certificates we can, right now. In the long run we might want to be more clever about only touching ones that need maintenance, but this will do for a start.

Most likely this should be run under cron.

Definition at line 1166 of file myrpki.py.

**13.145.3.21 def rpki.myrpki.main.entitydb\_complete ( *self*, *prefix*, *text*, *line*, *begidx*, *endidx* )**

Completion helper for entitydb filenames.

Definition at line 1048 of file myrpki.py.

**13.145.3.22 def rpki.myrpki.main.help\_overview ( *self* )**

Show program `__doc__` string. Perhaps there's some clever way to do this using the `textwrap` module, but for now something simple and crude will suffice.

Definition at line 1038 of file myrpki.py.

**13.145.3.23 def rpki.myrpki.main.read\_config ( *self* )**

Definition at line 1059 of file myrpki.py.

**13.145.3.24 def rpki.myrpki.main.renew\_children\_common ( *self*, *arg*, *plural* )**

Common code for `renew_child` and `renew_all_children` commands.

Definition at line 1521 of file myrpki.py.

#### 13.145.4 Member Data Documentation

##### 13.145.4.1 rpki.myrpki.main.bpki\_resources

Definition at line 1059 of file myrpki.py.

##### 13.145.4.2 rpki.myrpki.main.bpki\_servers

Definition at line 1059 of file myrpki.py.

##### 13.145.4.3 rpki.myrpki.main.cfg

Definition at line 1059 of file myrpki.py.

##### 13.145.4.4 rpki.myrpki.main.cfg\_file

Definition at line 1016 of file myrpki.py.

##### 13.145.4.5 rpki.myrpki.main.completedefault = rpki.cli.Cmd.filename\_ - complete [static]

Definition at line 1012 of file myrpki.py.

##### 13.145.4.6 rpki.myrpki.main.default\_repository

Definition at line 1059 of file myrpki.py.

##### 13.145.4.7 rpki.myrpki.main.entitydb

Definition at line 1059 of file myrpki.py.



#### 13.145.4.8 rpki.myrpki.main.handle

Definition at line 1059 of file myrpki.py.

#### 13.145.4.9 rpki.myrpki.main.histfile

Reimplemented from [rpki.cli.Cmd](#).

Definition at line 1059 of file myrpki.py.

#### 13.145.4.10 string rpki.myrpki.main.prompt = "myrpki> " [static]

Definition at line 1010 of file myrpki.py.

#### 13.145.4.11 rpki.myrpki.main.pubd\_contact\_info

Definition at line 1059 of file myrpki.py.

#### 13.145.4.12 rpki.myrpki.main.rsync\_module

Definition at line 1059 of file myrpki.py.

#### 13.145.4.13 rpki.myrpki.main.rsync\_server

Definition at line 1059 of file myrpki.py.

#### 13.145.4.14 rpki.myrpki.main.run\_pubd

Definition at line 1059 of file myrpki.py.

#### 13.145.4.15 rpki.myrpki.main.run\_rootd

Definition at line 1059 of file myrpki.py.

#### 13.145.4.16 rpki.myrpki.main.run\_rpkid

Definition at line 1059 of file myrpki.py.

#### 13.145.4.17 rpki.myrpki.main.show\_xml = False [static]

Definition at line 1014 of file myrpki.py.

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

- [myrpki.py \(3793\)](#)

### 13.146 rpki.myrpki.parent Class Reference

Inheritance diagram for rpki.myrpki.parent:

Collaboration diagram for rpki.myrpki.parent:

#### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [\\_\\_repr\\_\\_](#)
- def [add](#)
- def [xml](#)

#### Public Attributes

- [bpki\\_cms\\_certificate](#)
- [handle](#)
- [myhandle](#)
- [service\\_uri](#)
- [sia\\_base](#)

### 13.146.1 Detailed Description

Representation of one parent entity.

Definition at line 293 of file myrpki.py.

### 13.146.2 Constructor & Destructor Documentation

#### 13.146.2.1 `def rpki.myrpki.parent.__init__( self, handle )`

Definition at line 298 of file myrpki.py.

### 13.146.3 Member Function Documentation

#### 13.146.3.1 `def rpki.myrpki.parent.__repr__( self )`

Definition at line 305 of file myrpki.py.

#### 13.146.3.2 `def rpki.myrpki.parent.add ( self, service_uri = None, bpki_cms_certificate = None, myhandle = None, sia_base = None )`

Add service URI or BPKI certificates to this parent object.

Definition at line 317 of file myrpki.py.

#### 13.146.3.3 `def rpki.myrpki.parent.xml ( self, e )`

Render this parent object to XML.

Definition at line 333 of file myrpki.py.

### 13.146.4 Member Data Documentation

#### 13.146.4.1 `rpki.myrpki.parent.bpki_cms_certificate`

Definition at line 298 of file myrpki.py.

#### 13.146.4.2 rpki.myrpki.parent.handle

Definition at line 298 of file myrpki.py.

#### 13.146.4.3 rpki.myrpki.parent.myhandle

Definition at line 298 of file myrpki.py.

#### 13.146.4.4 rpki.myrpki.parent.service\_uri

Definition at line 298 of file myrpki.py.

#### 13.146.4.5 rpki.myrpki.parent.sia\_base

Definition at line 298 of file myrpki.py.

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

- [myrpki.py \(3793\)](#)

### 13.147 rpki.myrpki.parents Class Reference

Inheritance diagram for rpki.myrpki.parents:

Collaboration diagram for rpki.myrpki.parents:

#### Public Member Functions

- def [add](#)
- def [from\\_entitydb](#)
- def [xml](#)

#### 13.147.1 Detailed Description

Database of parent objects.

Definition at line 350 of file myrpki.py.

### 13.147.2 Member Function Documentation

**13.147.2.1** `def rpki.myrpki.parents.add ( self, handle, service_uri = None, bpki_cms_certificate = None, myhandle = None, sia_base = None )`

Add service URI or certificates to parent object, creating it if necessary.

Definition at line 355 of file myrpki.py.

**13.147.2.2** `def rpki.myrpki.parents.from_entitydb ( cls, fxcert, entitydb )`

Parse parent data from entitydb.

Definition at line 375 of file myrpki.py.

**13.147.2.3** `def rpki.myrpki.parents.xml ( self, e )`

Definition at line 370 of file myrpki.py.

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

- [myrpki.py \(3793\)](#)

## 13.148 rpki.myrpki.repositories Class Reference

Inheritance diagram for rpki.myrpki.repositories:

Collaboration diagram for rpki.myrpki.repositories:

### Public Member Functions

- `def add`
- `def from\_entitydb`
- `def xml`

### 13.148.1 Detailed Description

Database of repository objects.

Definition at line 437 of file myrpki.py.

### 13.148.2 Member Function Documentation

**13.148.2.1** `def rpki.myrpki.repositories.add ( self, handle, service_uri = None, bpk_certificate = None )`

Add service URI or certificate to repository object, creating it if necessary.

Definition at line 442 of file myrpki.py.

**13.148.2.2** `def rpki.myrpki.repositories.from_entitydb ( cls, fxcert, entitydb )`

Parse repository data from entitydb.

Definition at line 458 of file myrpki.py.

**13.148.2.3** `def rpki.myrpki.repositories.xml ( self, e )`

Definition at line 453 of file myrpki.py.

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

- [myrpki.py \(3793\)](#)

## 13.149 rpki.myrpki.repository Class Reference

Inheritance diagram for rpki.myrpki.repository:

Collaboration diagram for rpki.myrpki.repository:

### Public Member Functions

- [def \\_\\_init\\_\\_](#)
- [def \\_\\_repr\\_\\_](#)
- [def add](#)
- [def xml](#)

### Public Attributes

- [bpki\\_certificate](#)
- [handle](#)
- [service\\_uri](#)

#### 13.149.1 Detailed Description

Representation of one repository entity.

Definition at line 395 of file myrpki.py.

#### 13.149.2 Constructor & Destructor Documentation

##### 13.149.2.1 `def rpki.myrpki.repository.__init__( self, handle )`

Definition at line 400 of file myrpki.py.

#### 13.149.3 Member Function Documentation

##### 13.149.3.1 `def rpki.myrpki.repository.__repr__( self )`

Definition at line 405 of file myrpki.py.

##### 13.149.3.2 `def rpki.myrpki.repository.add ( self, service_uri = None, bpki_certificate = None )`

Add service URI or BPKI certificates to this repository object.

Definition at line 413 of file myrpki.py.

##### 13.149.3.3 `def rpki.myrpki.repository.xml ( self, e )`

Render this repository object to XML.

Definition at line 422 of file myrpki.py.

#### 13.149.4 Member Data Documentation

##### 13.149.4.1 rpki.myrpki.repository.bpki\_certificate

Definition at line 400 of file myrpki.py.

##### 13.149.4.2 rpki.myrpki.repository.handle

Definition at line 400 of file myrpki.py.

##### 13.149.4.3 rpki.myrpki.repository.service\_uri

Definition at line 400 of file myrpki.py.

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

- [myrpki.py \(3793\)](#)

#### 13.150 rpki.myrpki.roa\_request Class Reference

Inheritance diagram for rpki.myrpki.roa\_request:

Collaboration diagram for rpki.myrpki.roa\_request:

##### Public Member Functions

- [def \\_\\_init\\_\\_](#)
- [def \\_\\_repr\\_\\_](#)
- [def add](#)
- [def xml](#)

##### Public Attributes

- [asn](#)
- [group](#)
- [v4](#)
- [v6](#)



**Static Public Attributes**

- tuple **v4re** = re.compile("^[0-9]{1,3}\.){3}[0-9]{1,3}/[0-9]+(-[0-9]+)?\$", re.I)
- tuple **v6re** = re.compile("^[0-9a-f]{0,4:}{0,15}[0-9a-f]{0,4}/[0-9]+(-[0-9]+)?\$", re.I)

**13.150.1 Detailed Description**

Representation of a ROA request.

Definition at line 112 of file myrpki.py.

**13.150.2 Constructor & Destructor Documentation****13.150.2.1 def rpki.myrpki.roa\_request.\_\_init\_\_( self, asn, group )**

Definition at line 120 of file myrpki.py.

**13.150.3 Member Function Documentation****13.150.3.1 def rpki.myrpki.roa\_request.\_\_repr\_\_( self )**

Definition at line 126 of file myrpki.py.

**13.150.3.2 def rpki.myrpki.roa\_request.add( self, prefix )**

Add one prefix to this ROA request.

Definition at line 134 of file myrpki.py.

**13.150.3.3 def rpki.myrpki.roa\_request.xml( self, e )**

Generate XML element representing this ROA request.

Definition at line 145 of file myrpki.py.

#### 13.150.4 Member Data Documentation

##### 13.150.4.1 rpki.myrpki.roa\_request.asn

Definition at line 120 of file myrpki.py.

##### 13.150.4.2 rpki.myrpki.roa\_request.group

Definition at line 120 of file myrpki.py.

##### 13.150.4.3 rpki.myrpki.roa\_request.v4

Definition at line 120 of file myrpki.py.

```
13.150.4.4 tuple rpki.myrpki.roa_request.v4re = re.compile("^[0-9]{1,3}\.){3}[0-9]{1,3}/[0-9]+(-[0-9]+)?$", re.I)
[static]
```

Definition at line 117 of file myrpki.py.

##### 13.150.4.5 rpki.myrpki.roa\_request.v6

Definition at line 120 of file myrpki.py.

```
13.150.4.6 tuple rpki.myrpki.roa_request.v6re = re.compile("^[0-9a-f]{0,4}:{0,15}[0-9a-f]{0,4}/[0-9]+(-[0-9]+)?$", re.I)
[static]
```

Definition at line 118 of file myrpki.py.

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

- [myrpki.py \(3793\)](#)

## 13.151 rpki.myrpki.roa\_requests Class Reference

Inheritance diagram for rpki.myrpki.roa\_requests:

Collaboration diagram for rpki.myrpki.roa\_requests:

### Public Member Functions

- def [add](#)
- def [from\\_csv](#)
- def [xml](#)

#### 13.151.1 Detailed Description

Database of ROA requests.

Definition at line 155 of file myrpki.py.

#### 13.151.2 Member Function Documentation

##### 13.151.2.1 def rpki.myrpki.roa\_requests.add ( *self*, *asn*, *group*, *prefix* )

Add one <ASN, group, prefix> set to ROA request database.

Definition at line 160 of file myrpki.py.

##### 13.151.2.2 def rpki.myrpki.roa\_requests.from\_csv ( *cls*, *roa\_csv\_file* )

Parse ROA requests from CSV file.

Definition at line 177 of file myrpki.py.

##### 13.151.2.3 def rpki.myrpki.roa\_requests.xml ( *self*, *e* )

Render ROA requests as XML elements.

Definition at line 169 of file myrpki.py.

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

- [myrpki.py \(3793\)](#)

### 13.152 rpki.pubd.main Class Reference

Inheritance diagram for rpki.pubd.main:

Collaboration diagram for rpki.pubd.main:

#### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [client\\_handler](#)
- def [control\\_handler](#)
- def [handler\\_common](#)
- def [main](#)

#### Public Attributes

- [bpki\\_ta](#)
- [cfg](#)
- [cfg\\_file](#)
- [http\\_server\\_host](#)
- [http\\_server\\_port](#)
- [irbe\\_cert](#)
- [profile](#)
- [pubd\\_cert](#)
- [pubd\\_key](#)
- [publication\\_base](#)
- [publication\\_multimodule](#)
- [sql](#)

#### Static Public Attributes

- tuple [client\\_url\\_regexp](#) = re.compile("/client/([-A-Z0-9\_]+)\$", re.I)

#### 13.152.1 Detailed Description

Main program for pubd.

Definition at line 44 of file rpki/pubd.py.

### 13.152.2 Constructor & Destructor Documentation

#### 13.152.2.1 `def rpki.pubd.main.__init__ ( self )`

Definition at line 49 of file rpki/pubd.py.

#### 13.152.2.2 `def rpki.pubd.main.main ( self )`

Definition at line 79 of file rpki/pubd.py.

### 13.152.3 Member Function Documentation

#### 13.152.3.1 `def rpki.pubd.main.client_handler ( self, query, path, cb )`

Process one PDU from a client.

Definition at line 141 of file rpki/pubd.py.

#### 13.152.3.2 `def rpki.pubd.main.control_handler ( self, query, path, cb )`

Process one PDU from the IRBE.

Definition at line 121 of file rpki/pubd.py.

#### 13.152.3.3 `def rpki.pubd.main.handler_common ( self, query, client, cb, certs, crl = None )`

Common PDU handler code.

Definition at line 108 of file rpki/pubd.py.

#### 13.152.4 Member Data Documentation

##### 13.152.4.1 rpki.pubd.main.bpki\_ta

Definition at line 79 of file rpki/pubd.py.

##### 13.152.4.2 rpki.pubd.main.cfg

Definition at line 79 of file rpki/pubd.py.

##### 13.152.4.3 rpki.pubd.main.cfg\_file

Definition at line 49 of file rpki/pubd.py.

**13.152.4.4** `tuple rpki.pubd.main.client_url_regexp =  
re.compile("/client/([-A-Z0-9_]+)$", re.I) [static]`

Definition at line 139 of file rpki/pubd.py.

##### 13.152.4.5 rpki.pubd.main.http\_server\_host

Definition at line 79 of file rpki/pubd.py.

##### 13.152.4.6 rpki.pubd.main.http\_server\_port

Definition at line 79 of file rpki/pubd.py.

##### 13.152.4.7 rpki.pubd.main.irbe\_cert

Definition at line 79 of file rpki/pubd.py.

**13.152.4.8 `rpki.pubd.main.profile`**

Definition at line 49 of file `rpki/pubd.py`.

**13.152.4.9 `rpki.pubd.main.pubd_cert`**

Definition at line 79 of file `rpki/pubd.py`.

**13.152.4.10 `rpki.pubd.main.pubd_key`**

Definition at line 79 of file `rpki/pubd.py`.

**13.152.4.11 `rpki.pubd.main.publication_base`**

Definition at line 79 of file `rpki/pubd.py`.

**13.152.4.12 `rpki.pubd.main.publication_multimodule`**

Definition at line 79 of file `rpki/pubd.py`.

**13.152.4.13 `rpki.pubd.main.sql`**

Definition at line 79 of file `rpki/pubd.py`.

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

- [rpki/pubd.py \(3793\)](#)

**13.153 `rpki.publication.certificate_elt` Class Reference**

Inheritance diagram for `rpki.publication.certificate_elt`:

Collaboration diagram for `rpki.publication.certificate_elt`:

### Static Public Attributes

- string [element\\_name](#) = "certificate"
- [payload\\_type](#) = [rpki.x509.X509](#)

#### 13.153.1 Detailed Description

<certificate/> element.

Definition at line 271 of file publication.py.

#### 13.153.2 Member Data Documentation

##### 13.153.2.1 string [rpki.publication.certificate\\_elt.element\\_name](#) = "certificate" [static]

Definition at line 276 of file publication.py.

##### 13.153.2.2 [rpki.publication.certificate\\_elt.payload\\_type](#) = [rpki.x509.X509](#) [static]

Reimplemented from [rpki.publication.publication\\_object\\_elt](#).

Definition at line 277 of file publication.py.

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

- [publication.py](#) (3793)

## 13.154 rpki.publication.client\_elt Class Reference

Inheritance diagram for [rpki.publication.client\\_elt](#):

Collaboration diagram for [rpki.publication.client\\_elt](#):

### Public Member Functions

- def [check\\_allowed\\_uri](#)
- def [serve\\_fetch\\_all](#)
- def [serve\\_fetch\\_one\\_maybe](#)



**Static Public Attributes**

- tuple `attributes` = ("action", "tag", "client\_handle", "base\_uri")  
*XML attributes for this element.*
- `base_uri` = None
- `bpki_cert` = None
- `bpki_glue` = None
- string `element_name` = "client"
- tuple `elements` = ("bpki\_cert", "bpki\_glue")  
*XML elements contained by this element.*
- tuple `sql_template`

**13.154.1 Detailed Description**

`<client/>` element.

Definition at line 113 of file `publication.py`.

**13.154.2 Member Function Documentation****13.154.2.1 def rpki.publication.client\_elt.check\_allowed\_uri ( self, uri )**

Definition at line 144 of file `publication.py`.

**13.154.2.2 def rpki.publication.client\_elt.serve\_fetch\_all ( self )**

Find client objects on which a list method should operate.

Definition at line 138 of file `publication.py`.

**13.154.2.3 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 131 of file `publication.py`.

### 13.154.3 Member Data Documentation

**13.154.3.1** `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.

**13.154.3.2** `rpki.publication.client_elt.base_uri = None [static]`

Definition at line 127 of file publication.py.

**13.154.3.3** `rpki.publication.client_elt.bpki_cert = None [static]`

Definition at line 128 of file publication.py.

**13.154.3.4** `rpki.publication.client_elt.bpki_glue = None [static]`

Definition at line 129 of file publication.py.

**13.154.3.5** `string rpki.publication.client_elt.element_name = "client" [static]`

Definition at line 118 of file publication.py.

**13.154.3.6** `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.

### 13.154.3.7 tuple rpki.publication.client\_elt.sql\_template [static]

**Initial value:**

```
rpki.sql.template("client", "client_id", "client_handle", "base_uri",
 ("bpki_cert", rpki.x509.X509),
 ("bpki_glue", rpki.x509.X509),
 ("last_cms_timestamp", rpki.sundial.datetime))
```

Definition at line 122 of file publication.py.

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

- [publication.py \(3793\)](#)

## 13.155 rpki.publication.cms\_msg Class Reference

Inheritance diagram for rpki.publication.cms\_msg:

Collaboration diagram for rpki.publication.cms\_msg:

### Static Public Attributes

- string [encoding](#) = "us-ascii"
- [saxify](#) = sax\_handler.saxify
- [schema](#) = [rpki.relaxng.publication](#)

### 13.155.1 Detailed Description

Class to hold a CMS-signed publication PDU.

Definition at line 409 of file publication.py.

### 13.155.2 Member Data Documentation

#### 13.155.2.1 string rpki.publication.cms\_msg.encoding = "us-ascii" [static]

Definition at line 414 of file publication.py.

### 13.155.2.2 rpki.publication.cms\_msg.saxify = sax\_handler.saxify [static]

Reimplemented in [irbe\\_cli.publication cms\\_msg](#).

Definition at line 416 of file publication.py.

### 13.155.2.3 rpki.publication.cms\_msg.schema = rpki.relaxng.publication [static]

Definition at line 415 of file publication.py.

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

- [publication.py \(3793\)](#)

## 13.156 rpki.publication.config\_elt Class Reference

Inheritance diagram for rpki.publication.config\_elt:

Collaboration diagram for rpki.publication.config\_elt:

### Public Member Functions

- def [fetch](#)
- def [serve\\_fetch\\_one\\_maybe](#)
- def [serve\\_set](#)
- def [startElement](#)

### Public Attributes

- [config\\_id](#)

### Static Public Attributes

- tuple [attributes](#) = ("action", "tag")  
*XML attributes for this element.*
- string [element\\_name](#) = "config"
- tuple [elements](#) = ("bpki\_crl",)  
*XML elements contained by this element.*

- tuple `sql_template` = `rpki.sql.template`("config", "config\_id", ("bpki\_crl", rpki.x509.CRL))
- int `wired_in_config_id` = 1

### 13.156.1 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.

### 13.156.2 Member Function Documentation

#### 13.156.2.1 def rpki.publication.config\_elt.fetch ( *cls*, *gctx* )

Fetch the config object from SQL. This requires special handling because of the weird way we treat config\_id.

Definition at line 89 of file publication.py.

#### 13.156.2.2 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.

#### 13.156.2.3 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.

#### 13.156.2.4 `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.

#### 13.156.3 Member Data Documentation

##### 13.156.3.1 `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.

##### 13.156.3.2 `rpki.publication.config_elt.config_id`

Definition at line 83 of file publication.py.

##### 13.156.3.3 `string rpki.publication.config_elt.element_name = "config" [static]`

Definition at line 73 of file publication.py.

##### 13.156.3.4 `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.

```
13.156.3.5 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.

```
13.156.3.6 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 \(3793\)](#)

## 13.157 rpki.publication.control\_elt Class Reference

Inheritance diagram for rpki.publication.control\_elt:

Collaboration diagram for rpki.publication.control\_elt:

### Public Member Functions

- def [serve\\_dispatch](#)

### 13.157.1 Detailed Description

Virtual class for control channel objects.

Definition at line 47 of file publication.py.

### 13.157.2 Member Function Documentation

```
13.157.2.1 def rpki.publication.control_elt.serve_dispatch (self, r_msg, cb,
eb)
```

Action dispatch handler. This needs special handling because we need to make sure that this PDU arrived via the control channel.

Reimplemented from [rpki.xml\\_utils.data\\_elt](#).

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

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

- [publication.py](#) (3793)

### 13.158 `rpki.publication.crl_elt` Class Reference

Inheritance diagram for `rpki.publication.crl_elt`:

Collaboration diagram for `rpki.publication.crl_elt`:

#### Static Public Attributes

- string `element_name` = "crl"
- `payload_type` = `rpki.x509.CRL`

#### 13.158.1 Detailed Description

<crl/> element.

Definition at line 279 of file `publication.py`.

#### 13.158.2 Member Data Documentation

##### 13.158.2.1 string `rpki.publication.crl_elt.element_name` = "crl" `[static]`

Definition at line 284 of file `publication.py`.

##### 13.158.2.2 `rpki.publication.crl_elt.payload_type` = `rpki.x509.CRL` `[static]`

Reimplemented from [rpki.publication.publication\\_object\\_elt](#).

Definition at line 285 of file `publication.py`.

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

- [publication.py](#) (3793)



## 13.159 rpki.publication.ghostbuster\_elt Class Reference

Inheritance diagram for rpki.publication.ghostbuster\_elt:

Collaboration diagram for rpki.publication.ghostbuster\_elt:

### Static Public Attributes

- string [element\\_name](#) = "ghostbuster"
- [payload\\_type](#) = [rpki.x509.Ghostbuster](#)

#### 13.159.1 Detailed Description

```
<ghostbuster/> element.
```

Definition at line 303 of file publication.py.

#### 13.159.2 Member Data Documentation

##### 13.159.2.1 string rpki.publication.ghostbuster\_elt.element\_name = "ghostbuster" [static]

Definition at line 308 of file publication.py.

##### 13.159.2.2 rpki.publication.ghostbuster\_elt.payload\_type = rpki.x509.Ghostbuster [static]

Reimplemented from [rpki.publication.publication\\_object\\_elt](#).

Definition at line 309 of file publication.py.

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

- [publication.py \(3793\)](#)

## 13.160 rpki.publication.manifest\_elt Class Reference

Inheritance diagram for rpki.publication.manifest\_elt:

Collaboration diagram for rpki.publication.manifest\_elt:

### Static Public Attributes

- string [element\\_name](#) = "manifest"
- [payload\\_type](#) = [rpki.x509.SignedManifest](#)

#### 13.160.1 Detailed Description

<manifest/> element.

Definition at line 287 of file publication.py.

#### 13.160.2 Member Data Documentation

##### 13.160.2.1 string [rpki.publication.manifest\\_elt.element\\_name](#) = "manifest" [static]

Definition at line 292 of file publication.py.

##### 13.160.2.2 [rpki.publication.manifest\\_elt.payload\\_type](#) = [rpki.x509.SignedManifest](#) [static]

Reimplemented from [rpki.publication.publication\\_object\\_elt](#).

Definition at line 293 of file publication.py.

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

- [publication.py](#) (3793)

### 13.161 rpki.publication.msg Class Reference

Inheritance diagram for [rpki.publication.msg](#):

Collaboration diagram for [rpki.publication.msg](#):

### Public Member Functions

- def [serve\\_top\\_level](#)

**Static Public Attributes**

- tuple [pdus](#)  
*Dispatch table of PDUs for this protocol.*
- int [version](#) = 1  
*Protocol version.*

**13.161.1 Detailed Description**

Publication PDU.

Definition at line 356 of file publication.py.

**13.161.2 Member Function Documentation****13.161.2.1 def rpki.publication.msg.serve\_top\_level ( self, gctx, client, cb )**

Serve one msg PDU.

Definition at line 370 of file publication.py.

**13.161.3 Member Data Documentation****13.161.3.1 rpki::publication.msg::pdus [static]**

**Initial value:**

```
dict((x.element_name, x) for x in
 (config_elt, client_elt, certificate_elt, crl_elt, manifest_elt, ro
 a_elt, ghostbuster_elt, report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented in [irbe\\_cli.publication\\_msg](#).

Definition at line 367 of file publication.py.

**13.161.3.2 rpki::publication.msg::version = 1 [static]**

Protocol version.

Reimplemented from [rpki.xml\\_utils.msg](#).

Definition at line 363 of file publication.py.

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

- [publication.py \(3793\)](#)

## 13.162 rpki.publication.publication\_namespace Class Reference

Inheritance diagram for rpki.publication.publication\_namespace:

Collaboration diagram for rpki.publication.publication\_namespace:

### Static Public Attributes

- dictionary `nsmap` = { None : [xmlns](#) }
- string `xmlns` = "http://www.hactrn.net/uris/rpki/publication-spec/"

### 13.162.1 Detailed Description

XML namespace parameters for publication protocol.

Definition at line 39 of file publication.py.

### 13.162.2 Member Data Documentation

#### 13.162.2.1 dictionary `rpki.publication.publication_namespace.nsmap` = { None : `xmlns` } [static]

Definition at line 45 of file publication.py.

#### 13.162.2.2 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 \(3793\)](#)

## 13.163 rpki.publication.publication\_object\_elt Class Reference

Inheritance diagram for rpki.publication.publication\_object\_elt:

Collaboration diagram for rpki.publication.publication\_object\_elt:

### Public Member Functions

- def [endElement](#)
- def [make\\_publish](#)
- def [make\\_withdraw](#)
- def [raise\\_if\\_error](#)
- def [serve\\_dispatch](#)
- def [serve\\_publish](#)
- def [serve\\_withdraw](#)
- def [toXML](#)
- def [uri\\_to\\_filename](#)

### Static Public Attributes

- tuple [attributes](#) = ("action", "tag", "client\_handle", "uri")  
*XML attributes for this element.*
- [payload](#) = None
- [payload\\_type](#) = None

#### 13.163.1 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 148 of file publication.py.

#### 13.163.2 Member Function Documentation

##### 13.163.2.1 def rpki.publication.publication\_object\_elt.endElement ( *self*, *stack*, *name*, *text* )

Handle a publishable element element.

Reimplemented from [rpki.xml\\_utils.base\\_elt](#).

Definition at line 162 of file publication.py.

**13.163.2.2** `def rpki.publication.publication_object_elt.make_publish ( cls,  
uri, obj, tag = None )`

Construct a publication PDU.

Definition at line 250 of file publication.py.

**13.163.2.3** `def rpki.publication.publication_object_elt.make_withdraw ( cls,  
uri, obj, tag = None )`

Construct a withdrawal PDU.

Definition at line 258 of file publication.py.

**13.163.2.4** `def rpki.publication.publication_object_elt.raise_if_error ( self )`

No-op, since this is not a <report\_error/> PDU.

Definition at line 265 of file publication.py.

**13.163.2.5** `def rpki.publication.publication_object_elt.serve_dispatch ( self,  
r_msg, cb, eb )`

Action dispatch handler.

Definition at line 180 of file publication.py.

**13.163.2.6** `def rpki.publication.publication_object_elt.serve_publish ( self )`

Publish an object.

Definition at line 205 of file publication.py.

**13.163.2.7** `def rpki.publication.publication_object_elt.serve_withdraw ( self )`

Withdraw an object.

Definition at line 220 of file publication.py.

**13.163.2.8** `def rpki.publication.publication_object_elt.toXML ( self )`

Generate XML element for publishable object.

Reimplemented from [rpki.xml\\_utils.base\\_elt](#).

Definition at line 171 of file publication.py.

**13.163.2.9** `def rpki.publication.publication_object_elt.uri_to_filename ( self )`

Convert a URI to a local filename.

Definition at line 234 of file publication.py.

**13.163.3 Member Data Documentation****13.163.3.1** `tuple rpki.publication.publication_object_elt.attributes = ("action", "tag", "client_handle", "uri") [static]`

XML attributes for this element.

Reimplemented from [rpki.xml\\_utils.base\\_elt](#).

Definition at line 158 of file publication.py.

### 13.163.3.2 rpki.publication.publication\_object\_elt.payload = None [static]

Definition at line 160 of file publication.py.

### 13.163.3.3 rpki.publication.publication\_object\_elt.payload\_type = None [static]

Reimplemented in [rpki.publication.certificate\\_elt](#), [rpki.publication.crl\\_elt](#), [rpki.publication.manifest\\_elt](#), [rpki.publication.roa\\_elt](#), and [rpki.publication.ghostbuster\\_elt](#).

Definition at line 159 of file publication.py.

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

- [publication.py \(3793\)](#)

## 13.164 rpki.publication.report\_error\_elt Class Reference

Inheritance diagram for [rpki.publication.report\\_error\\_elt](#):

Collaboration diagram for [rpki.publication.report\\_error\\_elt](#):

### Public Member Functions

- def [\\_\\_str\\_\\_](#)
- def [from\\_exception](#)
- def [raise\\_if\\_error](#)

### Public Attributes

- [error\\_code](#)
- [tag](#)

### Static Public Attributes

- tuple [attributes](#) = ("tag", "[error\\_code](#)")  
*XML attributes for this element.*
- string [element\\_name](#) = "report\_error"
- [error\\_text](#) = None



- string `text_attribute` = "error\_text"  
*Name of the class attribute that holds the text value.*

#### 13.164.1 Detailed Description

<report\_error/> element.

Definition at line 315 of file publication.py.

#### 13.164.2 Member Function Documentation

##### 13.164.2.1 `def rpki.publication.report_error_elt.__str__( self )`

Convert a `base_elt` object to string format.

Reimplemented from `rpki.xml_utils.base_elt`.

Definition at line 337 of file publication.py.

##### 13.164.2.2 `def rpki.publication.report_error_elt.from_exception( cls, e, tag = None )`

Generate a <report\_error/> element from an exception.

Definition at line 327 of file publication.py.

##### 13.164.2.3 `def rpki.publication.report_error_elt.raise_if_error( self )`

Raise exception associated with this <report\_error/> PDU.

Definition at line 346 of file publication.py.

#### 13.164.3 Member Data Documentation

##### 13.164.3.1 `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 321 of file publication.py.

**13.164.3.2** `string rpki.publication.report_error_elt.element_name = "report_error" [static]`

Definition at line 320 of file publication.py.

**13.164.3.3** `rpki.publication.report_error_elt.error_code`

Definition at line 329 of file publication.py.

**13.164.3.4** `rpki.publication.report_error_elt.error_text = None [static]`

Definition at line 324 of file publication.py.

**13.164.3.5** `rpki.publication.report_error_elt.tag`

Definition at line 329 of file publication.py.

**13.164.3.6** `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 322 of file publication.py.

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

- [publication.py \(3793\)](#)

## 13.165 rpki.publication.roa\_elt Class Reference

Inheritance diagram for rpki.publication.roa\_elt:

Collaboration diagram for rpki.publication.roa\_elt:

### Static Public Attributes

- string [element\\_name](#) = "roa"
- [payload\\_type](#) = [rpki.x509.ROA](#)

#### 13.165.1 Detailed Description

```
<roa/> element.
```

Definition at line 295 of file publication.py.

#### 13.165.2 Member Data Documentation

##### 13.165.2.1 string rpki.publication.roa\_elt.element\_name = "roa" [static]

Definition at line 300 of file publication.py.

##### 13.165.2.2 rpki.publication.roa\_elt.payload\_type = rpki.x509.ROA [static]

Reimplemented from [rpki.publication.publication\\_object\\_elt](#).

Definition at line 301 of file publication.py.

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

- [publication.py](#) (3793)

## 13.166 rpki.publication.sax\_handler Class Reference

Inheritance diagram for rpki.publication.sax\_handler:

Collaboration diagram for rpki.publication.sax\_handler:

### Static Public Attributes

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

#### 13.166.1 Detailed Description

SAX handler for publication protocol.

Definition at line 400 of file `publication.py`.

#### 13.166.2 Member Data Documentation

##### 13.166.2.1 string `rpki.publication.sax_handler.name` = "msg" [static]

Definition at line 406 of file `publication.py`.

##### 13.166.2.2 `rpki.publication.sax_handler.pdu` = `msg` [static]

Reimplemented in `irbe_cli.publication_sax_handler`.

Definition at line 405 of file `publication.py`.

##### 13.166.2.3 string `rpki.publication.sax_handler.version` = "1" [static]

Definition at line 407 of file `publication.py`.

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

- `publication.py` (3793)

### 13.167 rpki.resource\_set.resource\_bag Class Reference

Inheritance diagram for `rpki.resource_set.resource_bag`:

Collaboration diagram for `rpki.resource_set.resource_bag`:

### Public Member Functions

- [def \\_\\_eq\\_\\_](#)
- [def \\_\\_init\\_\\_](#)
- [def \\_\\_ne\\_\\_](#)
- [def \\_\\_str\\_\\_](#)
- [def empty](#)
- [def from\\_inheritance](#)
- [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.*

#### 13.167.1 Detailed Description

Container to simplify passing around the usual triple of ASN, IPv4, and IPv6 resource sets.

Definition at line 665 of file resource\_set.py.

#### 13.167.2 Constructor & Destructor Documentation

**13.167.2.1** `def rpki.resource_set.resource_bag.__init__( self, asn = None, v4 = None, v6 = None, valid_until = None )`

Definition at line 683 of file resource\_set.py.

### 13.167.3 Member Function Documentation

#### 13.167.3.1 `def rpki.resource_set.resource_bag.__eq__( self, other )`

Definition at line 750 of file resource\_set.py.

#### 13.167.3.2 `def rpki.resource_set.resource_bag.__ne__( self, other )`

Definition at line 756 of file resource\_set.py.

#### 13.167.3.3 `def rpki.resource_set.resource_bag.__str__( self )`

Definition at line 779 of file resource\_set.py.

#### 13.167.3.4 `def rpki.resource_set.resource_bag.empty( self )`

True iff all resource sets in this bag are empty.

Definition at line 744 of file resource\_set.py.

#### 13.167.3.5 `def rpki.resource_set.resource_bag.from_inheritance( cls )`

Build a resource bag that just inherits everything from its parent.

Definition at line 706 of file resource\_set.py.

#### 13.167.3.6 `def rpki.resource_set.resource_bag.from_rfc3779_tuples( cls, exts )`

Build a resource\_bag from intermediate form generated by RFC 3779 ASN.1 decoder.

Definition at line 721 of file resource\_set.py.

**13.167.3.7 def rpki.resource\_set.resource\_bag.intersection ( self, other )**

Compute intersection with another resource\_bag. valid\_until attribute (if any) inherits from self.

Definition at line 759 of file resource\_set.py.

**13.167.3.8 def rpki.resource\_set.resource\_bag.oversized ( self, other )**

True iff self is oversized with respect to other.

Definition at line 689 of file resource\_set.py.

**13.167.3.9 def rpki.resource\_set.resource\_bag.undersized ( self, other )**

True iff self is undersized with respect to other.

Definition at line 697 of file resource\_set.py.

**13.167.3.10 def rpki.resource\_set.resource\_bag.union ( self, other )**

Compute union with another resource\_bag. valid\_until attribute (if any) inherits from self.

Definition at line 769 of file resource\_set.py.

**13.167.4 Member Data Documentation****13.167.4.1 rpki::resource\_set.resource\_bag::asn**

Set of Autonomous System Number resources.

Definition at line 683 of file resource\_set.py.

#### 13.167.4.2 rpki::resource\_set.resource\_bag::v4

Set of IPv4 resources.

Definition at line 683 of file resource\_set.py.

#### 13.167.4.3 rpki::resource\_set.resource\_bag::v6

Set of IPv6 resources.

Definition at line 683 of file resource\_set.py.

#### 13.167.4.4 rpki::resource\_set.resource\_bag::valid\_until

Expiration date of resources, for setting certificate notAfter field.

Definition at line 683 of file resource\_set.py.

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

- [resource\\_set.py \(3688\)](#)

### 13.168 rpki.resource\_set.resource\_range Class Reference

Inheritance diagram for rpki.resource\_set.resource\_range:

Collaboration diagram for rpki.resource\_set.resource\_range:

#### Public Member Functions

- [def \\_\\_cmp\\_\\_](#)
- [def \\_\\_init\\_\\_](#)

#### Public Attributes

- [max](#)
- [min](#)



### 13.168.1 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 55 of file resource\_set.py.

### 13.168.2 Constructor & Destructor Documentation

#### 13.168.2.1 def rpki.resource\_set.resource\_range.\_\_init\_\_( self, min, max )

Initialize and sanity check a resource\_range.

Definition at line 64 of file resource\_set.py.

### 13.168.3 Member Function Documentation

#### 13.168.3.1 def rpki.resource\_set.resource\_range.\_\_cmp\_\_( self, other )

Compare two resource\_range objects.

Definition at line 73 of file resource\_set.py.

### 13.168.4 Member Data Documentation

#### 13.168.4.1 rpki.resource\_set.resource\_range.max

Definition at line 66 of file resource\_set.py.

#### 13.168.4.2 rpki.resource\_set.resource\_range.min

Reimplemented in [rpki.resource\\_set.resource\\_range\\_as](#).

Definition at line 66 of file resource\_set.py.

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

- [resource\\_set.py \(3688\)](#)

### 13.169 rpki.resource\_set.resource\_range\_as Class Reference

Inheritance diagram for rpki.resource\_set.resource\_range\_as:

Collaboration diagram for rpki.resource\_set.resource\_range\_as:

#### Public Member Functions

- def [\\_\\_str\\_\\_](#)
- def [from\\_strings](#)
- def [parse\\_str](#)
- def [to\\_rfc3779\\_tuple](#)

#### Public Attributes

- [min](#)

#### Static Public Attributes

- [datum\\_type](#) = [long](#)  
*Type of underlying data (min and max).*

#### 13.169.1 Detailed Description

Range of Autonomous System Numbers.

Denotes a single ASN by a range whose min and max values are identical.

Definition at line 80 of file resource\_set.py.

#### 13.169.2 Member Function Documentation

##### 13.169.2.1 def rpki.resource\_set.resource\_range\_as.\_\_str\_\_( self )

Convert a resource\_range\_as to string format.

Definition at line 93 of file resource\_set.py.

**13.169.2.2** `def rpki.resource_set.resource_range_as.from_strings ( cls, a, b = None )`

Construct ASN range from strings.

Definition at line 123 of file resource\_set.py.

**13.169.2.3** `def rpki.resource_set.resource_range_as.parse_str ( cls, x )`

Parse ASN resource range from text (eg, XML attributes).

Definition at line 112 of file resource\_set.py.

**13.169.2.4** `def rpki.resource_set.resource_range_as.to_rfc3779_tuple ( self )`

Convert a resource\_range\_as to tuple format for RFC 3779 ASN.1 encoding.

Definition at line 102 of file resource\_set.py.

### 13.169.3 Member Data Documentation

**13.169.3.1** `rpki::resource_set.resource_range_as::datum_type = long`  
`[static]`

Type of underlying data (min and max).

Definition at line 91 of file resource\_set.py.

**13.169.3.2** `rpki.resource_set.resource_range_as.min`

Reimplemented from [rpki.resource\\_set.resource\\_range](#).

Definition at line 95 of file resource\_set.py.

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

- [resource\\_set.py \(3688\)](#)

## 13.170 rpki.resource\_set.resource\_range\_ip Class Reference

Inheritance diagram for rpki.resource\_set.resource\_range\_ip:

Collaboration diagram for rpki.resource\_set.resource\_range\_ip:

### Public Member Functions

- def [\\_\\_str\\_\\_](#)
- def [chop\\_into\\_prefixes](#)
- def [from\\_strings](#)
- def [make\\_prefix](#)
- def [parse\\_str](#)
- def [prefixlen](#)
- def [to\\_rfc3779\\_tuple](#)

### Static Private Attributes

- [\\_prefixlen](#) = prefixlen

#### 13.170.1 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 131 of file resource\_set.py.

#### 13.170.2 Member Function Documentation

##### 13.170.2.1 def rpki.resource\_set.resource\_range\_ip.\_\_str\_\_( self )

Convert a resource\_range\_ip to string format.

Definition at line 162 of file resource\_set.py.

**13.170.2.2** `def rpki.resource_set.resource_range_ip.chop_into_prefixes ( self, result )`

Chop up a resource\_range\_ip into ranges that can be represented as prefixes.

Definition at line 207 of file resource\_set.py.

**13.170.2.3** `def rpki.resource_set.resource_range_ip.from_strings ( cls, a, b = None )`

Construct IP address range from strings.

Definition at line 231 of file resource\_set.py.

**13.170.2.4** `def rpki.resource_set.resource_range_ip.make_prefix ( cls, prefix, prefixlen )`

Construct a resource range corresponding to a prefix.

Definition at line 197 of file resource\_set.py.

**13.170.2.5** `def rpki.resource_set.resource_range_ip.parse_str ( cls, x )`

Parse IP address range or prefix from text (eg, XML attributes).

Definition at line 184 of file resource\_set.py.

**13.170.2.6** `def rpki.resource_set.resource_range_ip.prefixlen ( self )`

Determine whether a resource\_range\_ip can be expressed as a prefix. Returns prefix length if it can, otherwise raises MustBePrefix exception.

Definition at line 142 of file resource\_set.py.

### 13.170.2.7 def rpki.resource\_set.resource\_range\_ip.to\_rfc3779\_tuple ( self )

Convert a resource\_range\_ip to tuple format for RFC 3779 ASN.1 encoding.

Definition at line 171 of file resource\_set.py.

### 13.170.3 Member Data Documentation

#### 13.170.3.1 rpki.resource\_set.resource\_range\_ip.\_prefixlen = prefixlen [static, private]

Definition at line 160 of file resource\_set.py.

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

- [resource\\_set.py \(3688\)](#)

## 13.171 rpki.resource\_set.resource\_range\_ipv4 Class Reference

Inheritance diagram for rpki.resource\_set.resource\_range\_ipv4:

Collaboration diagram for rpki.resource\_set.resource\_range\_ipv4:

### Static Public Attributes

- [datum\\_type = rpki.ipaddrs.v4addr](#)  
*Type of underlying data (min and max).*

### 13.171.1 Detailed Description

Range of IPv4 addresses.

Definition at line 250 of file resource\_set.py.

### 13.171.2 Member Data Documentation

#### 13.171.2.1 rpki::resource\_set.resource\_range\_ipv4::datum\_type = rpki.ipaddrs.v4addr [static]

Type of underlying data (min and max).

Definition at line 258 of file resource\_set.py.

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

- [resource\\_set.py \(3688\)](#)

### 13.172 rpki.resource\_set.resource\_range\_ipv6 Class Reference

Inheritance diagram for rpki.resource\_set.resource\_range\_ipv6:

Collaboration diagram for rpki.resource\_set.resource\_range\_ipv6:

#### Static Public Attributes

- [datum\\_type = rpki.ipaddrs.v6addr](#)  
*Type of underlying data (min and max).*

### 13.172.1 Detailed Description

Range of IPv6 addresses.

Definition at line 260 of file resource\_set.py.

### 13.172.2 Member Data Documentation

#### 13.172.2.1 rpki::resource\_set.resource\_range\_ipv6::datum\_type = rpki.ipaddrs.v6addr [static]

Type of underlying data (min and max).

Definition at line 268 of file resource\_set.py.

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

- [resource\\_set.py \(3688\)](#)

## 13.173 rpki.resource\_set.resource\_set Class Reference

Inheritance diagram for rpki.resource\_set.resource\_set:

Collaboration diagram for rpki.resource\_set.resource\_set:

### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [\\_\\_str\\_\\_](#)
- def [append](#)
- def [canonize](#)
- def [contains](#)
- def [difference](#)
- def [extend](#)
- def [from\\_sql](#)
- def [intersection](#)
- def [issubset](#)
- def [issuperset](#)
- def [parse\\_str](#)
- def [symmetric\\_difference](#)
- def [union](#)

### Static Public Attributes

- [canonical](#) = False  
*Whether this [resource\\_set](#) is currently in canonical form.*
- [inherit](#) = False  
*Boolean indicating whether this [resource\\_set](#) uses RFC 3779 inheritance.*

### Private Member Functions

- def [\\_comm](#)

#### 13.173.1 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 286 of file resource\_set.py.



### 13.173.2 Constructor & Destructor Documentation

#### 13.173.2.1 def rpki.resource\_set.resource\_set.\_\_init\_\_ ( self, ini = None )

Initialize a resource\_set.

Definition at line 304 of file resource\_set.py.

### 13.173.3 Member Function Documentation

#### 13.173.3.1 def rpki.resource\_set.resource\_set.\_\_str\_\_ ( self )

Convert a resource\_set to string format.

Definition at line 353 of file resource\_set.py.

#### 13.173.3.2 def rpki.resource\_set.resource\_set.\_comm ( self, other ) [private]

Like comm(1), sort of.

Returns a tuple of three resource sets: resources only in self, resources only in other, and resources in both. Used (not very efficiently) as the basis for most set operations on resource sets.

Definition at line 362 of file resource\_set.py.

#### 13.173.3.3 def rpki.resource\_set.resource\_set.append ( self, item )

Wrapper around list.append() (q.v.) to reset canonical flag.

Definition at line 339 of file resource\_set.py.

#### 13.173.3.4 def rpki.resource\_set.resource\_set.canonize ( self )

Whack this resource\_set into canonical form.

Definition at line 323 of file resource\_set.py.

#### 13.173.3.5 def rpki.resource\_set.resource\_set.contains ( self, item )

Set membership test for resource sets.

Definition at line 447 of file resource\_set.py.

#### 13.173.3.6 def rpki.resource\_set.resource\_set.difference ( self, other )

Set difference for resource sets.

Definition at line 434 of file resource\_set.py.

#### 13.173.3.7 def rpki.resource\_set.resource\_set.extend ( self, item )

Wrapper around list.extend() (q.v.) to reset canonical flag.

Definition at line 346 of file resource\_set.py.

#### 13.173.3.8 def rpki.resource\_set.resource\_set.from\_sql ( cls, sql, query, args = None )

Create resource set from an SQL query.

sql is an object that supports execute() and fetchall() methods like a DB API 2.0 cursor object.

query is an SQL query that returns a sequence of (min, max) pairs.

Definition at line 487 of file resource\_set.py.

**13.173.3.9** `def rpki.resource_set.resource_set.intersection ( self, other )`

Set intersection for resource sets.

Definition at line 428 of file `resource_set.py`.

**13.173.3.10** `def rpki.resource_set.resource_set.issubset ( self, other )`

Test whether `self` is a subset (possibly improper) of `other`.

Definition at line 471 of file `resource_set.py`.

**13.173.3.11** `def rpki.resource_set.resource_set.issuperset ( self, other )`

Test whether `self` is a superset (possibly improper) of `other`.

Definition at line 480 of file `resource_set.py`.

**13.173.3.12** `def rpki.resource_set.resource_set.parse_str ( cls, s )`

Parse resource set from text string (eg, XML attributes). This is a backwards compatability wrapper, real functionality is now part of the range classes.

Definition at line 503 of file `resource_set.py`.

**13.173.3.13** `def rpki.resource_set.resource_set.symmetric_difference ( self,  
other )`

Set symmetric difference (XOR) for resource sets.

Definition at line 440 of file `resource_set.py`.

### 13.173.3.14 def rpki.resource\_set.resource\_set.union ( self, other )

Set union for resource sets.

Definition at line 396 of file resource\_set.py.

### 13.173.4 Member Data Documentation

#### 13.173.4.1 rpki::resource\_set.resource\_set::canonical = False [static]

Whether this [resource\\_set](#) is currently in canonical form.

Definition at line 302 of file resource\_set.py.

#### 13.173.4.2 rpki::resource\_set.resource\_set::inherit = False [static]

Boolean indicating whether this [resource\\_set](#) uses RFC 3779 inheritance.

Reimplemented in [rpki.resource\\_set.resource\\_set\\_as](#), and [rpki.resource\\_set.resource\\_set\\_ip](#).

Definition at line 297 of file resource\_set.py.

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

- [resource\\_set.py](#) (3688)

### 13.174 rpki.resource\_set.resource\_set\_as Class Reference

Inheritance diagram for rpki.resource\_set.resource\_set\_as:

Collaboration diagram for rpki.resource\_set.resource\_set\_as:

#### Public Member Functions

- def [parse\\_rfc3779\\_tuple](#)
- 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](#).*

### 13.174.1 Detailed Description

Autonomous System Number resource set.

Definition at line 511 of file resource\_set.py.

### 13.174.2 Member Function Documentation

#### 13.174.2.1 `def rpki.resource_set.resource_set_as.parse_rfc3779_tuple ( self, x )`

Parse ASN resource from tuple format generated by RFC 3779 ASN.1 decoder.

Definition at line 521 of file resource\_set.py.

#### 13.174.2.2 `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 539 of file resource\_set.py.

### 13.174.3 Member Data Documentation

#### 13.174.3.1 `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 524 of file resource\_set.py.

### 13.174.3.2 rpki::resource\_set.resource\_set\_as::range\_type = resource\_range\_as [static]

Type of range underlying this type of [resource\\_set](#).

Definition at line 519 of file resource\_set.py.

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

- [resource\\_set.py](#) (3688)

## 13.175 rpki.resource\_set.resource\_set\_ip Class Reference

Inheritance diagram for rpki.resource\_set.resource\_set\_ip:

Collaboration diagram for rpki.resource\_set.resource\_set\_ip:

### Public Member Functions

- def [parse\\_rfc3779\\_tuple](#)
- def [to\\_rfc3779\\_tuple](#)
- def [to\\_roa\\_prefix\\_set](#)

### Public Attributes

- [inherit](#)

*Boolean indicating whether this [resource\\_set](#) uses RFC 3779 inheritance.*

### 13.175.1 Detailed Description

(Generic) IP address resource set.

This is a virtual class. You probably don't want to use it directly.

Definition at line 552 of file resource\_set.py.

### 13.175.2 Member Function Documentation

#### 13.175.2.1 `def rpki.resource_set.resource_set_ip.parse_rfc3779_tuple ( self, x )`

Parse IP address resource sets from tuple format generated by RFC 3779 ASN.1 decoder.

Definition at line 560 of file resource\_set.py.

#### 13.175.2.2 `def rpki.resource_set.resource_set_ip.to_rfc3779_tuple ( self )`

Convert IP resource set into tuple format used by RFC 3779 ASN.1 encoder.

Definition at line 589 of file resource\_set.py.

#### 13.175.2.3 `def rpki.resource_set.resource_set_ip.to_roa_prefix_set ( self )`

Convert from a resource set to a ROA prefix set.

Definition at line 578 of file resource\_set.py.

### 13.175.3 Member Data Documentation

#### 13.175.3.1 `rpki.resource_set.resource_set_ip.inherit`

Boolean indicating whether this [resource\\_set](#) uses RFC 3779 inheritance.

Reimplemented from [rpki.resource\\_set.resource\\_set](#).

Definition at line 563 of file resource\_set.py.

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

- [resource\\_set.py \(3688\)](#)

## 13.176 rpki.resource\_set.resource\_set\_ipv4 Class Reference

Inheritance diagram for rpki.resource\_set.resource\_set\_ipv4:

Collaboration diagram for rpki.resource\_set.resource\_set\_ipv4:

### Static Public Attributes

- string `afi` = "\x00\x01"  
*Address Family Identifier value for IPv4.*
- `range_type` = `resource_range_ipv4`  
*Type of range underlying this type of `resource_set`.*

### 13.176.1 Detailed Description

IPv4 address resource set.

Definition at line 602 of file `resource_set.py`.

### 13.176.2 Member Data Documentation

#### 13.176.2.1 `rpki::resource_set.resource_set_ipv4::afi = "\x00\x01" [static]`

Address Family Identifier value for IPv4.

Definition at line 615 of file `resource_set.py`.

#### 13.176.2.2 `rpki::resource_set.resource_set_ipv4::range_type = resource_range_ipv4 [static]`

Type of range underlying this type of `resource_set`.

Definition at line 610 of file `resource_set.py`.

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

- `resource_set.py` (3688)



## 13.177 rpki.resource\_set.resource\_set\_ipv6 Class Reference

Inheritance diagram for rpki.resource\_set.resource\_set\_ipv6:

Collaboration diagram for rpki.resource\_set.resource\_set\_ipv6:

### Static Public Attributes

- string `afi` = "\x00\x02"  
*Address Family Identifier value for IPv6.*
- `range_type` = `resource_range_ipv6`  
*Type of range underlying this type of `resource_set`.*

### 13.177.1 Detailed Description

IPv6 address resource set.

Definition at line 617 of file `resource_set.py`.

### 13.177.2 Member Data Documentation

#### 13.177.2.1 `rpki::resource_set.resource_set_ipv6::afi = "\x00\x02" [static]`

Address Family Identifier value for IPv6.

Definition at line 630 of file `resource_set.py`.

#### 13.177.2.2 `rpki::resource_set.resource_set_ipv6::range_type = resource_range_ipv6 [static]`

Type of range underlying this type of `resource_set`.

Definition at line 625 of file `resource_set.py`.

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

- `resource_set.py` (3688)

## 13.178 rpki.resource\_set.roa\_prefix Class Reference

Inheritance diagram for rpki.resource\_set.roa\_prefix:

Collaboration diagram for rpki.resource\_set.roa\_prefix:

### Public Member Functions

- def [\\_\\_cmp\\_\\_](#)
- def [\\_\\_init\\_\\_](#)
- def [\\_\\_str\\_\\_](#)
- def [from\\_roa\\_tuple](#)
- def [max](#)
- def [min](#)
- def [parse\\_str](#)
- def [to\\_resource\\_range](#)
- def [to\\_roa\\_tuple](#)

### Public Attributes

- [max\\_prefixlen](#)  
*Maximum prefix length.*
- [prefix](#)  
*The prefix itself, an IP address with bits beyond the prefix length zeroed.*
- [prefixlen](#)  
*(Minimum) prefix length.*

### 13.178.1 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 801 of file `resource_set.py`.

### 13.178.2 Constructor & Destructor Documentation

#### 13.178.2.1 `def rpki.resource_set.roa_prefix.__init__( self, prefix, prefixlen, max_prefixlen = None )`

Initialize a ROA prefix. max\_prefixlen is optional and defaults to prefixlen. max\_prefixlen must not be smaller than prefixlen.

Definition at line 820 of file resource\_set.py.

### 13.178.3 Member Function Documentation

#### 13.178.3.1 `def rpki.resource_set.roa_prefix.__cmp__( self, other )`

Compare two ROA prefix objects. Comparision is based on prefix, prefixlen, and max\_prefixlen, in that order.

Definition at line 832 of file resource\_set.py.

#### 13.178.3.2 `def rpki.resource_set.roa_prefix.__str__( self )`

Convert a ROA prefix to string format.

Definition at line 842 of file resource\_set.py.

#### 13.178.3.3 `def rpki.resource_set.roa_prefix.from_roa_tuple( cls, o )`

Convert from ROA ASN.1 tuple format.

Definition at line 894 of file resource\_set.py.

#### 13.178.3.4 `def rpki.resource_set.roa_prefix.max( self )`

Return highest address covered by prefix.

Definition at line 865 of file resource\_set.py.

**13.178.3.5 def rpki.resource\_set.roa\_prefix.min ( self )**

Return lowest address covered by prefix.

Definition at line 859 of file resource\_set.py.

**13.178.3.6 def rpki.resource\_set.roa\_prefix.parse\_str ( cls, x )**

Parse ROA prefix from text (eg, an XML attribute).

Definition at line 881 of file resource\_set.py.

**13.178.3.7 def rpki.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 851 of file resource\_set.py.

**13.178.3.8 def rpki.resource\_set.roa\_prefix.to\_roa\_tuple ( self )**

Convert a resource\_range\_ip to tuple format for ROA ASN.1 encoding.

Definition at line 872 of file resource\_set.py.

**13.178.4 Member Data Documentation****13.178.4.1 rpki::resource\_set.roa\_prefix::max\_prefixlen**

Maximum prefix length.

Definition at line 823 of file resource\_set.py.

#### 13.178.4.2 rpki::resource\_set.roa\_prefix::prefix

The prefix itself, an IP address with bits beyond the prefix length zeroed.

Definition at line 823 of file resource\_set.py.

#### 13.178.4.3 rpki::resource\_set.roa\_prefix::prefixlen

(Minimum) prefix length.

Definition at line 823 of file resource\_set.py.

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

- [resource\\_set.py \(3688\)](#)

### 13.179 rpki.resource\_set.roa\_prefix\_ipv4 Class Reference

Inheritance diagram for rpki.resource\_set.roa\_prefix\_ipv4:

Collaboration diagram for rpki.resource\_set.roa\_prefix\_ipv4:

#### Static Public Attributes

- [range\\_type = resource\\_range\\_ipv4](#)  
*Type of corresponding [resource\\_range\\_ip](#).*

#### 13.179.1 Detailed Description

IPv4 ROA prefix.

Definition at line 901 of file resource\_set.py.

#### 13.179.2 Member Data Documentation

**13.179.2.1** `rpki::resource_set.roa_prefix_ipv4::range_type = resource_range_ipv4 [static]`

Type of corresponding [resource\\_range\\_ip](#).

Definition at line 909 of file resource\_set.py.

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

- [resource\\_set.py](#) (3688)

### 13.180 rpki.resource\_set.roa\_prefix\_ipv6 Class Reference

Inheritance diagram for rpki.resource\_set.roa\_prefix\_ipv6:

Collaboration diagram for rpki.resource\_set.roa\_prefix\_ipv6:

#### Static Public Attributes

- `range_type = resource_range_ipv6`  
*Type of corresponding [resource\\_range\\_ip](#).*

#### 13.180.1 Detailed Description

IPv6 ROA prefix.

Definition at line 911 of file resource\_set.py.

#### 13.180.2 Member Data Documentation

##### 13.180.2.1 rpki::resource\_set.roa\_prefix\_ipv6::range\_type = resource\_range\_ipv6 [static]

Type of corresponding [resource\\_range\\_ip](#).

Definition at line 919 of file resource\_set.py.

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

- [resource\\_set.py](#) (3688)

### 13.181 rpki.resource\_set.roa\_prefix\_set Class Reference

Inheritance diagram for rpki.resource\_set.roa\_prefix\_set:

Collaboration diagram for rpki.resource\_set.roa\_prefix\_set:

### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [\\_\\_str\\_\\_](#)
- def [from\\_sql](#)
- def [parse\\_str](#)
- def [to\\_resource\\_set](#)
- def [to\\_roa\\_tuple](#)

#### 13.181.1 Detailed Description

Set of ROA prefixes, analogous to the `resource_set_ip` class.

Definition at line 921 of file `resource_set.py`.

#### 13.181.2 Constructor & Destructor Documentation

##### 13.181.2.1 def rpki.resource\_set.roa\_prefix\_set.\_\_init\_\_( self, ini = None )

Initialize a ROA prefix set.

Definition at line 926 of file `resource_set.py`.

#### 13.181.3 Member Function Documentation

##### 13.181.3.1 def rpki.resource\_set.roa\_prefix\_set.\_\_str\_\_( self )

Convert a ROA prefix set to string format.

Definition at line 939 of file `resource_set.py`.

##### 13.181.3.2 def rpki.resource\_set.roa\_prefix\_set.from\_sql( cls, sql, query, args = None )

Create ROA prefix set from an SQL query.

`sql` is an object that supports `execute()` and `fetchall()` methods like a DB API 2.0 cursor object.

query is an SQL query that returns a sequence of (prefix, prefixlen, max\_prefixlen) triples.

Definition at line 971 of file resource\_set.py.

### 13.181.3.3 def rpki.resource\_set.roa\_prefix\_set.parse\_str ( cls, s )

Parse ROA prefix from text (eg, an XML attribute).  
This method is a backwards compatability shim.

Definition at line 946 of file resource\_set.py.

### 13.181.3.4 def rpki.resource\_set.roa\_prefix\_set.to\_resource\_set ( self )

Convert a ROA prefix set to a resource set. This is an irreversable transformation. We have to compute a union here because ROA prefix sets can include overlaps, while RFC 3779 resource sets cannot. This is ugly, and there is almost certainly a more efficient way to do this, but start by getting the output right before worrying about making it fast or pretty.

Definition at line 953 of file resource\_set.py.

### 13.181.3.5 def rpki.resource\_set.roa\_prefix\_set.to\_roa\_tuple ( self )

Convert ROA prefix set into tuple format used by ROA ASN.1 encoder. This is a variation on the format used in RFC 3779.

Definition at line 986 of file resource\_set.py.

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

- [resource\\_set.py \(3688\)](#)

## 13.182 rpki.resource\_set.roa\_prefix\_set\_ipv4 Class Reference

Inheritance diagram for rpki.resource\_set.roa\_prefix\_set\_ipv4:

Collaboration diagram for rpki.resource\_set.roa\_prefix\_set\_ipv4:



### Static Public Attributes

- `prefix_type = roa_prefix_ipv4`  
*Type of underlying [roa\\_prefix](#).*
- `resource_set_type = resource_set_ipv4`  
*Type of corresponding [resource\\_set\\_ip](#) class.*

#### 13.182.1 Detailed Description

Set of IPv4 ROA prefixes.

Definition at line 996 of file `resource_set.py`.

#### 13.182.2 Member Data Documentation

##### 13.182.2.1 `rpki::resource_set.roa_prefix_set_ipv4::prefix_type = roa_prefix_ipv4` `[static]`

Type of underlying [roa\\_prefix](#).

Definition at line 1004 of file `resource_set.py`.

##### 13.182.2.2 `rpki::resource_set.roa_prefix_set_ipv4::resource_set_type = resource_set_ipv4` `[static]`

Type of corresponding [resource\\_set\\_ip](#) class.

Definition at line 1009 of file `resource_set.py`.

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

- [resource\\_set.py](#) (3688)

### 13.183 rpki.resource\_set.roa\_prefix\_set\_ipv6 Class Reference

Inheritance diagram for `rpki.resource_set.roa_prefix_set_ipv6`:

Collaboration diagram for `rpki.resource_set.roa_prefix_set_ipv6`:

**Static Public Attributes**

- [prefix\\_type](#) = [roa\\_prefix\\_ipv6](#)  
*Type of underlying [roa\\_prefix](#).*
- [resource\\_set\\_type](#) = [resource\\_set\\_ipv6](#)  
*Type of corresponding [resource\\_set\\_ip](#) class.*

**13.183.1 Detailed Description**

Set of IPv6 ROA prefixes.

Definition at line 1014 of file `resource_set.py`.

**13.183.2 Member Data Documentation****13.183.2.1 rpki::resource\_set.roa\_prefix\_set\_ipv6::prefix\_type = roa\_prefix\_ipv6 [static]**

Type of underlying [roa\\_prefix](#).

Definition at line 1022 of file `resource_set.py`.

**13.183.2.2 rpki::resource\_set.roa\_prefix\_set\_ipv6::resource\_set\_type = resource\_set\_ipv6 [static]**

Type of corresponding [resource\\_set\\_ip](#) class.

Definition at line 1027 of file `resource_set.py`.

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

- [resource\\_set.py](#) (3688)

**13.184 rpki.roa.ROAIPAddress Class Reference**

Inheritance diagram for `rpki.roa.ROAIPAddress`:

Collaboration diagram for `rpki.roa.ROAIPAddress`:

#### Public Member Functions

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

#### Public Attributes

- [address](#)
- [maxLength](#)

#### 13.184.1 Detailed Description

Definition at line 47 of file roa.py.

#### 13.184.2 Constructor & Destructor Documentation

**13.184.2.1** `def rpki.roa.ROAIPAddress.__init__( self, optional = 0, default = "" )`

Definition at line 48 of file roa.py.

#### 13.184.3 Member Data Documentation

##### 13.184.3.1 rpki.roa.ROAIPAddress.address

Definition at line 48 of file roa.py.

##### 13.184.3.2 rpki.roa.ROAIPAddress.maxLength

Definition at line 48 of file roa.py.

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

- [roa.py \(3598\)](#)

#### 13.185 rpki.roa.ROAIPAddresses Class Reference

Inheritance diagram for rpki.roa.ROAIPAddresses:

Collaboration diagram for rpki.roa.ROAIPAddresses:

### Public Member Functions

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

#### 13.185.1 Detailed Description

Definition at line 54 of file roa.py.

#### 13.185.2 Constructor & Destructor Documentation

**13.185.2.1** `def rpki.roa.ROAIPAddresses.__init__( self, optional = 0, default = " )`

Definition at line 55 of file roa.py.

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

- [roa.py \(3598\)](#)

### 13.186 rpki.roa.ROAIPAddressFamilies Class Reference

Inheritance diagram for rpki.roa.ROAIPAddressFamilies:

Collaboration diagram for rpki.roa.ROAIPAddressFamilies:

### Public Member Functions

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

#### 13.186.1 Detailed Description

Definition at line 65 of file roa.py.

#### 13.186.2 Constructor & Destructor Documentation

**13.186.2.1** `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 \(3598\)](#)

## 13.187 rpki.roa.ROAIPAddressFamily Class Reference

Inheritance diagram for rpki.roa.ROAIPAddressFamily:

Collaboration diagram for rpki.roa.ROAIPAddressFamily:

### Public Member Functions

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

### Public Attributes

- [addresses](#)
- [addressFamily](#)

#### 13.187.1 Detailed Description

Definition at line 58 of file roa.py.

#### 13.187.2 Constructor & Destructor Documentation

**13.187.2.1** `def rpki.roa.ROAIPAddressFamily.__init__ ( self, optional = 0, default = " )`

Definition at line 59 of file roa.py.

#### 13.187.3 Member Data Documentation

##### 13.187.3.1 rpki.roa.ROAIPAddressFamily.addresses

Definition at line 59 of file roa.py.

### 13.187.3.2 rpki.roa.ROAIPAddressFamily.addressFamily

Definition at line 59 of file roa.py.

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

- [roa.py \(3598\)](#)

## 13.188 rpki.roa.RouteOriginAttestation Class Reference

Inheritance diagram for rpki.roa.RouteOriginAttestation:

Collaboration diagram for rpki.roa.RouteOriginAttestation:

### Public Member Functions

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

### Public Attributes

- [asID](#)
- [explicitVersion](#)
- [ipAddrBlocks](#)
- [version](#)

### 13.188.1 Detailed Description

Definition at line 69 of file roa.py.

### 13.188.2 Constructor & Destructor Documentation

#### 13.188.2.1 `def rpki.roa.RouteOriginAttestation.__init__( self, optional = 0, default = " )`

Definition at line 70 of file roa.py.

### 13.188.3 Member Data Documentation

#### 13.188.3.1 rpki.roa.RouteOriginAttestation.asID

Definition at line 70 of file roa.py.

#### 13.188.3.2 rpki.roa.RouteOriginAttestation.explicitVersion

Definition at line 70 of file roa.py.

#### 13.188.3.3 rpki.roa.RouteOriginAttestation.ipAddrBlocks

Definition at line 70 of file roa.py.

#### 13.188.3.4 rpki.roa.RouteOriginAttestation.version

Definition at line 70 of file roa.py.

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

- [roa.py \(3598\)](#)

### 13.189 rpki.rootd.cms\_msg Class Reference

Inheritance diagram for rpki.rootd.cms\_msg:

Collaboration diagram for rpki.rootd.cms\_msg:

#### Static Public Attributes

- [saxify](#) = sax\_handler.saxify

#### 13.189.1 Detailed Description

Definition at line 93 of file rpki/rootd.py.

### 13.189.2 Member Data Documentation

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

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

Definition at line 94 of file `rpki/rootd.py`.

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

- [rpki/rootd.py \(3793\)](#)

## 13.190 rpki.rootd.issue\_pdu Class Reference

Inheritance diagram for `rpki.rootd.issue_pdu`:

Collaboration diagram for `rpki.rootd.issue_pdu`:

### Public Member Functions

- def [serve\\_pdu](#)

### 13.190.1 Detailed Description

Definition at line 52 of file `rpki/rootd.py`.

### 13.190.2 Member Function Documentation

#### 13.190.2.1 def rpki.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 53 of file `rpki/rootd.py`.

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

- [rpki/rootd.py \(3793\)](#)



## 13.191 rpki.rootd.list\_pdu Class Reference

Inheritance diagram for rpki.rootd.list\_pdu:

Collaboration diagram for rpki.rootd.list\_pdu:

### Public Member Functions

- def [serve\\_pdu](#)

#### 13.191.1 Detailed Description

Definition at line 46 of file rpki/rootd.py.

#### 13.191.2 Member Function Documentation

##### 13.191.2.1 def rpki.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 47 of file rpki/rootd.py.

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

- [rpki/rootd.py \(3793\)](#)

## 13.192 rpki.rootd.main Class Reference

Inheritance diagram for rpki.rootd.main:

Collaboration diagram for rpki.rootd.main:

### Public Member Functions

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

#### Public Attributes

- [bpki\\_ta](#)
- [cfg](#)
- [cfg\\_file](#)
- [child\\_bpki\\_cert](#)
- [http\\_server\\_host](#)
- [http\\_server\\_port](#)
- [rootd\\_bpki\\_cert](#)
- [rootd\\_bpki\\_crl](#)
- [rootd\\_bpki\\_key](#)
- [rpki\\_base\\_uri](#)
- [rpki\\_class\\_name](#)
- [rpki\\_root\\_cert\\_file](#)
- [rpki\\_root\\_cert\\_uri](#)
- [rpki\\_root\\_crl](#)
- [rpki\\_root\\_dir](#)
- [rpki\\_root\\_key](#)
- [rpki\\_root\\_manifest](#)
- [rpki\\_subject\\_cert](#)
- [rpki\\_subject\\_lifetime](#)
- [rpki\\_subject\\_pkcs10](#)
- [rpki\\_subject\\_regen](#)

#### Static Public Attributes

- [rpki\\_root\\_cert](#) = None

#### 13.192.1 Detailed Description

Definition at line 96 of file rpki/rootd.py.

### 13.192.2 Constructor & Destructor Documentation

#### 13.192.2.1 def rpki.rootd.main.\_\_init\_\_ ( *self* )

Definition at line 262 of file rpki/rootd.py.

### 13.192.3 Member Function Documentation

#### 13.192.3.1 def rpki.rootd.main.compose\_response ( *self*, *r\_msg*, *pkcs10* = *None* )

Definition at line 223 of file rpki/rootd.py.

#### 13.192.3.2 def rpki.rootd.main.del\_subject\_cert ( *self* )

Definition at line 123 of file rpki/rootd.py.

#### 13.192.3.3 def rpki.rootd.main.del\_subject\_pkcs10 ( *self* )

Definition at line 142 of file rpki/rootd.py.

#### 13.192.3.4 def rpki.rootd.main.get\_root\_cert ( *self* )

Definition at line 100 of file rpki/rootd.py.

#### 13.192.3.5 def rpki.rootd.main.get\_subject\_cert ( *self* )

Definition at line 107 of file rpki/rootd.py.

#### 13.192.3.6 def rpki.rootd.main.get\_subject\_pkcs10 ( *self* )

Definition at line 128 of file rpki/rootd.py.

**13.192.3.7 def rpki.rootd.main.issue\_subject\_cert\_maybe ( *self*, *new\_pkcs10* )**

Definition at line 149 of file rpki/rootd.py.

**13.192.3.8 def rpki.rootd.main.root\_newer\_than\_subject ( *self* )**

Definition at line 104 of file rpki/rootd.py.

**13.192.3.9 def rpki.rootd.main.set\_subject\_cert ( *self*, *cert* )**

Definition at line 116 of file rpki/rootd.py.

**13.192.3.10 def rpki.rootd.main.set\_subject\_pkcs10 ( *self*, *pkcs10* )**

Definition at line 136 of file rpki/rootd.py.

**13.192.3.11 def rpki.rootd.main.up\_down\_handler ( *self*, *query*, *path*, *cb* )**

Definition at line 236 of file rpki/rootd.py.

**13.192.4 Member Data Documentation****13.192.4.1 rpki.rootd.main.bpki\_ta**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.2 rpki.rootd.main.cfg**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.3 rpki.rootd.main.cfg\_file**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.4 rpki.rootd.main.child\_bpki\_cert**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.5 rpki.rootd.main.http\_server\_host**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.6 rpki.rootd.main.http\_server\_port**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.7 rpki.rootd.main.rootd\_bpki\_cert**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.8 rpki.rootd.main.rootd\_bpki\_crl**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.9 rpki.rootd.main.rootd\_bpki\_key**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.10 rpki.rootd.main.rpki\_base\_uri**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.11 rpki.rootd.main.rpki\_class\_name**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.12 rpki.rootd.main.rpki\_root\_cert = None [static]**

Definition at line 98 of file rpki/rootd.py.

**13.192.4.13 rpki.rootd.main.rpki\_root\_cert\_file**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.14 rpki.rootd.main.rpki\_root\_cert\_uri**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.15 rpki.rootd.main.rpki\_root\_crl**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.16 rpki.rootd.main.rpki\_root\_dir**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.17 rpki.rootd.main.rpki\_root\_key**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.18 rpki.rootd.main.rpki\_root\_manifest**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.19 rpki.rootd.main.rpki\_subject\_cert**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.20 rpki.rootd.main.rpki\_subject\_lifetime**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.21 rpki.rootd.main.rpki\_subject\_pkcs10**

Definition at line 262 of file rpki/rootd.py.

**13.192.4.22 rpki.rootd.main.rpki\_subject\_regen**

Definition at line 262 of file rpki/rootd.py.

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

- [rpki/rootd.py \(3793\)](#)

**13.193 rpki.rootd.message\_pdu Class Reference**

Inheritance diagram for rpki.rootd.message\_pdu:

Collaboration diagram for rpki.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())`

**13.193.1 Detailed Description**

Definition at line 71 of file [rpki/rootd.py](#).

**13.193.2 Member Function Documentation****13.193.2.1 def [rpki.rootd.message\\_pdu.log\\_query](#) ( *self*, *child* )**

Log query we're handling.

Reimplemented from [rpki.up\\_down.message\\_pdu](#).

Definition at line 84 of file [rpki/rootd.py](#).

**13.193.3 Member Data Documentation****13.193.3.1 dictionary [rpki.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 73 of file [rpki/rootd.py](#).



### 13.193.3.2 `tuple rpki.rootd.message_pdu.type2name = dict((v, k) for k, v in name2type.items())` `[static]`

Reimplemented from [rpki.up\\_down.message\\_pdu](#).

Definition at line 82 of file `rpki/rootd.py`.

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

- [rpki/rootd.py \(3793\)](#)

## 13.194 `rpki.rootd.revoke_pdu` Class Reference

Inheritance diagram for `rpki.rootd.revoke_pdu`:

Collaboration diagram for `rpki.rootd.revoke_pdu`:

### Public Member Functions

- `def` [serve\\_pdu](#)

### 13.194.1 Detailed Description

Definition at line 59 of file `rpki/rootd.py`.

### 13.194.2 Member Function Documentation

#### 13.194.2.1 `def rpki.rootd.revoke_pdu.serve_pdu ( self, q_msg, r_msg, child, cb, eb )`

Serve one revoke request PDU.

Reimplemented from [rpki.up\\_down.revoke\\_pdu](#).

Definition at line 60 of file `rpki/rootd.py`.

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

- [rpki/rootd.py \(3793\)](#)

## 13.195 rpki.rootd.sax\_handler Class Reference

Inheritance diagram for rpki.rootd.sax\_handler:

Collaboration diagram for rpki.rootd.sax\_handler:

### Static Public Attributes

- [pdu](#) = [message\\_pdu](#)

### 13.195.1 Detailed Description

Definition at line 90 of file rpki/rootd.py.

### 13.195.2 Member Data Documentation

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

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

Definition at line 91 of file rpki/rootd.py.

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

- [rpki/rootd.py \(3793\)](#)

## 13.196 rpki.rpkid.ca\_detail\_obj Class Reference

Inheritance diagram for rpki.rpkid.ca\_detail\_obj:

Collaboration diagram for rpki.rpkid.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 [fetch\\_child\\_certs](#)
- def [generate\\_crl](#)
- def [generate\\_manifest](#)
- def [generate\\_manifest\\_cert](#)
- def [ghostbusters](#)
- def [has\\_expired](#)
- def [issue](#)
- def [issue\\_ee](#)
- def [manifest\\_published\\_callback](#)
- def [manifest\\_uri](#)
- def [reissue](#)
- 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](#)
- [private\\_key\\_id](#)
- [public\\_key](#)
- [state](#)

#### Static Public Attributes

- [crl\\_published](#) = None
- [latest\\_ca\\_cert](#) = None
- [manifest\\_published](#) = None
- tuple [sql\\_template](#)

#### 13.196.1 Detailed Description

Internal CA detail object.

Definition at line 653 of file rpki/rpkid.py.

### 13.196.2 Member Function Documentation

#### 13.196.2.1 `def rpki.rpkid.ca_detail_obj.activate ( self, ca, cert, uri, callback, errback, predecessor = None )`

Activate this ca\_detail.

Definition at line 755 of file rpki/rpkid.py.

#### 13.196.2.2 `def rpki.rpkid.ca_detail_obj.ca ( self )`

Fetch CA object to which this ca\_detail links.

Definition at line 688 of file rpki/rpkid.py.

#### 13.196.2.3 `def rpki.rpkid.ca_detail_obj.child_certs ( self )`

Fetch all child\_cert objects that link to this ca\_detail.

Definition at line 701 of file rpki/rpkid.py.

#### 13.196.2.4 `def rpki.rpkid.ca_detail_obj.create ( cls, ca )`

Create a new ca\_detail object for a specified CA.

Definition at line 913 of file rpki/rpkid.py.

#### 13.196.2.5 `def rpki.rpkid.ca_detail_obj.crl_published_callback ( self, pdu )`

Check result of CRL publication.

Definition at line 1036 of file rpki/rpkid.py.

**13.196.2.6** `def rpki.rpkid.ca_detail_obj.crl_uri ( self )`

Return publication URI for this ca\_detail's CRL.

Definition at line 729 of file rpki/rpkid.py.

**13.196.2.7** `def rpki.rpkid.ca_detail_obj.crl_uri_tail ( self )`

Return tail (filename portion) of publication URI for this ca\_detail's CRL.

Definition at line 736 of file rpki/rpkid.py.

**13.196.2.8** `def rpki.rpkid.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 782 of file rpki/rpkid.py.

**13.196.2.9** `def rpki.rpkid.ca_detail_obj.fetch_child_certs ( self, child = None,  
ski = None, unique = False )`

Fetch all child\_cert objects that link to this ca\_detail.

Definition at line 694 of file rpki/rpkid.py.

**13.196.2.10** `def rpki.rpkid.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 1000 of file rpki/rpkid.py.

**13.196.2.11** `def rpki.rpkid.ca_detail_obj.generate_manifest ( self, publisher, nextUpdate = None )`

Generate a new manifest for this ca\_detail.

Definition at line 1044 of file rpki/rpkid.py.

**13.196.2.12** `def rpki.rpkid.ca_detail_obj.generate_manifest_cert ( self )`

Generate a new manifest certificate for this ca\_detail.

Definition at line 948 of file rpki/rpkid.py.

**13.196.2.13** `def rpki.rpkid.ca_detail_obj.ghostbusters ( self )`

Fetch all Ghostbuster objects that link to this ca\_detail.

Definition at line 722 of file rpki/rpkid.py.

**13.196.2.14** `def rpki.rpkid.ca_detail_obj.has_expired ( self )`

Return whether this ca\_detail's certificate has expired.

Definition at line 749 of file rpki/rpkid.py.

**13.196.2.15** `def rpki.rpkid.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 956 of file rpki/rpkid.py.

**13.196.2.16** `def rpki.rpkid.ca_detail_obj.issue_ee ( self, ca, resources,  
subject_key, sia = None )`

Issue a new EE certificate.

Definition at line 931 of file rpki/rpkid.py.

**13.196.2.17** `def rpki.rpkid.ca_detail_obj.manifest_published_callback ( self,  
pdu )`

Check result of manifest publication.

Definition at line 1079 of file rpki/rpkid.py.

**13.196.2.18** `def rpki.rpkid.ca_detail_obj.manifest_uri ( self )`

Return publication URI for this ca\_detail's manifest.

Definition at line 743 of file rpki/rpkid.py.

**13.196.2.19** `def rpki.rpkid.ca_detail_obj.reissue ( self, cb, eb )`

Reissue all current certificates issued by this ca\_detail.

Definition at line 1087 of file rpki/rpkid.py.

**13.196.2.20** `def rpki.rpkid.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 816 of file rpki/rpkid.py.

#### 13.196.2.21 def rpki.rpkid.ca\_detail\_obj.revoked\_certs ( self )

Fetch all revoked\_cert objects that link to this ca\_detail.

Definition at line 708 of file rpki/rpkid.py.

#### 13.196.2.22 def rpki.rpkid.ca\_detail\_obj.roas ( self )

Fetch all ROA objects that link to this ca\_detail.

Definition at line 715 of file rpki/rpkid.py.

#### 13.196.2.23 def rpki.rpkid.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 679 of file rpki/rpkid.py.

#### 13.196.2.24 def rpki.rpkid.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 888 of file rpki/rpkid.py.

### **13.196.3 Member Data Documentation**

#### **13.196.3.1 rpki.rpkid.ca\_detail\_obj.ca\_cert\_uri**

Definition at line 757 of file rpki/rpkid.py.

#### **13.196.3.2 rpki.rpkid.ca\_detail\_obj.ca\_id**

Definition at line 915 of file rpki/rpkid.py.

#### **13.196.3.3 rpki.rpkid.ca\_detail\_obj.crl\_published = None [static]**

Definition at line 675 of file rpki/rpkid.py.

#### **13.196.3.4 rpki.rpkid.ca\_detail\_obj.gctx**

Reimplemented from [rpki.sql.sql\\_persistent](#).

Definition at line 915 of file rpki/rpkid.py.

#### **13.196.3.5 rpki.rpkid.ca\_detail\_obj.latest\_ca\_cert = None [static]**

Definition at line 677 of file rpki/rpkid.py.

#### **13.196.3.6 rpki.rpkid.ca\_detail\_obj.latest\_crl**

Definition at line 1004 of file rpki/rpkid.py.

**13.196.3.7 rpki.rpkid.ca\_detail\_obj.latest\_manifest**

Definition at line 1046 of file rpki/rpkid.py.

**13.196.3.8 rpki.rpkid.ca\_detail\_obj.latest\_manifest\_cert**

Definition at line 836 of file rpki/rpkid.py.

**13.196.3.9 rpki.rpkid.ca\_detail\_obj.manifest\_private\_key\_id**

Definition at line 836 of file rpki/rpkid.py.

**13.196.3.10 rpki.rpkid.ca\_detail\_obj.manifest\_public\_key**

Definition at line 836 of file rpki/rpkid.py.

**13.196.3.11 rpki.rpkid.ca\_detail\_obj.manifest\_published = None [static]**

Definition at line 676 of file rpki/rpkid.py.

**13.196.3.12 rpki.rpkid.ca\_detail\_obj.private\_key\_id**

Definition at line 836 of file rpki/rpkid.py.

**13.196.3.13 rpki.rpkid.ca\_detail\_obj.public\_key**

Definition at line 915 of file rpki/rpkid.py.

**13.196.3.14 tuple rpki.rpkid.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 658 of file rpki/rpkid.py.

### 13.196.3.15 rpki.rpkid.ca\_detail\_obj.state

Definition at line 757 of file rpki/rpkid.py.

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

- [rpki/rpkid.py \(3793\)](#)

## 13.197 rpki.rpkid.ca\_obj Class Reference

Inheritance diagram for rpki.rpkid.ca\_obj:

Collaboration diagram for rpki.rpkid.ca\_obj:

### Public Member Functions

- def [active\\_ca\\_detail](#)
- def [ca\\_details](#)
- def [check\\_for\\_updates](#)
- def [construct\\_sia\\_uri](#)
- def [create](#)
- def [delete](#)
- def [deprecated\\_ca\\_details](#)
- def [issue\\_response\\_candidate\\_ca\\_details](#)
- def [next\\_crl\\_number](#)
- def [next\\_manifest\\_number](#)

- def [next\\_serial\\_number](#)
- def [parent](#)
- def [pending\\_ca\\_details](#)
- def [reissue](#)
- def [rekey](#)
- def [revoke](#)
- def [revoked\\_ca\\_details](#)

#### 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](#)

#### 13.197.1 Detailed Description

Internal CA object.

Definition at line 360 of file rpki/rpkid.py.

#### 13.197.2 Member Function Documentation

##### 13.197.2.1 def rpki.rpkid.ca\_obj.active\_ca\_detail ( *self* )

Fetch the active ca\_detail for this CA, if any.

Definition at line 400 of file rpki/rpkid.py.

##### 13.197.2.2 def rpki.rpkid.ca\_obj.ca\_details ( *self* )

Fetch all ca\_detail objects that link to this CA object.

Definition at line 386 of file rpki/rpkid.py.

**13.197.2.3** `def rpki.rpkid.ca_obj.check_for_updates ( self, parent, rc, cb, eb )`

Parent has signaled continued existence 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 442 of file rpki/rpkid.py.

**13.197.2.4** `def rpki.rpkid.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 429 of file rpki/rpkid.py.

**13.197.2.5** `def rpki.rpkid.ca_obj.create ( cls, parent, rc, cb, eb )`

Parent has signaled existence of a new resource class, so we need to create and set up a corresponding CA object.

Definition at line 531 of file rpki/rpkid.py.

**13.197.2.6** `def rpki.rpkid.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 555 of file rpki/rpkid.py.

**13.197.2.7 def rpki.rpkid.ca\_obj.deprecated\_ca\_details ( self )**

Fetch deprecated ca\_details for this CA, if any.

Definition at line 407 of file rpki/rpkid.py.

**13.197.2.8 def rpki.rpkid.ca\_obj.issue\_response\_candidate\_ca\_details ( self )**

Fetch ca\_details which are candidates for consideration when processing an up-down issue\_response PDU.

Definition at line 421 of file rpki/rpkid.py.

**13.197.2.9 def rpki.rpkid.ca\_obj.next\_crl\_number ( self )**

Allocate a CRL serial number.

Definition at line 597 of file rpki/rpkid.py.

**13.197.2.10 def rpki.rpkid.ca\_obj.next\_manifest\_number ( self )**

Allocate a manifest serial number.

Definition at line 589 of file rpki/rpkid.py.

**13.197.2.11 def rpki.rpkid.ca\_obj.next\_serial\_number ( self )**

Allocate a certificate serial number.

Definition at line 581 of file rpki/rpkid.py.

**13.197.2.12 def rpki.rpkid.ca\_obj.parent ( self )**

Fetch parent object to which this CA object links.

Definition at line 379 of file rpki/rpkid.py.

**13.197.2.13 def rpki.rpkid.ca\_obj.pending\_ca\_details ( self )**

Fetch the pending ca\_details for this CA, if any.

Definition at line 393 of file rpki/rpkid.py.

**13.197.2.14 def rpki.rpkid.ca\_obj.reissue ( self, cb, eb )**

Reissue all current certificates issued by this CA.

Definition at line 642 of file rpki/rpkid.py.

**13.197.2.15 def rpki.rpkid.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 605 of file rpki/rpkid.py.

**13.197.2.16 def rpki.rpkid.ca\_obj.revoke ( self, cb, eb )**

Revoke deprecated ca\_detail objects associated with this ca.

Definition at line 630 of file rpki/rpkid.py.

**13.197.2.17 def rpki.rpkid.ca\_obj.revoked\_ca\_details ( self )**

Fetch revoked ca\_details for this CA, if any.

Definition at line 414 of file rpki/rpkid.py.

**13.197.3 Member Data Documentation****13.197.3.1 rpki.rpkid.ca\_obj.gctx**

Reimplemented from [rpki.sql.sql\\_persistent](#).

Definition at line 534 of file rpki/rpkid.py.

**13.197.3.2 int rpki.rpkid.ca\_obj.last\_crl\_sn = 0 [static]**

Definition at line 374 of file rpki/rpkid.py.

**13.197.3.3 int rpki.rpkid.ca\_obj.last\_issued\_sn = 0 [static]**

Definition at line 375 of file rpki/rpkid.py.

**13.197.3.4 int rpki.rpkid.ca\_obj.last\_manifest\_sn = 0 [static]**

Definition at line 376 of file rpki/rpkid.py.

**13.197.3.5 rpki.rpkid.ca\_obj.parent\_id**

Definition at line 534 of file rpki/rpkid.py.

**13.197.3.6 rpki.rpkid.ca\_obj.parent\_resource\_class**



Definition at line 534 of file rpki/rpkid.py.

### 13.197.3.7 rpki.rpkid.ca\_obj.sia\_uri

Definition at line 447 of file rpki/rpkid.py.

### 13.197.3.8 tuple rpki.rpkid.ca\_obj.sql\_template [static]

**Initial value:**

```
rpki.sql.template(
 "ca",
 "ca_id",
 "last_crl_sn",
 ("next_crl_update", rpki.sundial.datetime),
 "last_issued_sn", "last_manifest_sn",
 ("next_manifest_update", rpki.sundial.datetime),
 "sia_uri", "parent_id", "parent_resource_class")
```

Definition at line 365 of file rpki/rpkid.py.

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

- [rpki/rpkid.py \(3793\)](#)

## 13.198 rpki.rpkid.child\_cert\_obj Class Reference

Inheritance diagram for rpki.rpkid.child\_cert\_obj:

Collaboration diagram for rpki.rpkid.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](#)

#### 13.198.1 Detailed Description

Certificate that has been issued to a child.

Definition at line 1101 of file rpki/rpkid.py.

#### 13.198.2 Constructor & Destructor Documentation

**13.198.2.1** `def rpki.rpkid.child_cert_obj.__init__( self, gctx = None, child_id = None, ca_detail_id = None, cert = None )`

Initialize a child\_cert\_obj.

Definition at line 1115 of file rpki/rpkid.py.

#### 13.198.3 Member Function Documentation

**13.198.3.1** `def rpki.rpkid.child_cert_obj.ca_detail( self )`

Fetch ca\_detail object to which this child\_cert object links.

Definition at line 1136 of file rpki/rpkid.py.

**13.198.3.2 def rpki.rpkid.child\_cert\_obj.child ( self )**

Fetch child object to which this child\_cert object links.

Definition at line 1129 of file rpki/rpkid.py.

**13.198.3.3 def rpki.rpkid.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 1254 of file rpki/rpkid.py.

**13.198.3.4 def rpki.rpkid.child\_cert\_obj.published\_callback ( self, pdu )**

Publication callback: check result and mark published.

Definition at line 1286 of file rpki/rpkid.py.

**13.198.3.5 def rpki.rpkid.child\_cert\_obj.reissue ( self, ca\_detail, publisher, resources = None, sia = None, force = False )**

Reissue an existing child cert, reusing the public key. If the child cert we would generate is identical to the one we already have, we just return the one we already have. If we have to revoke the old child cert when generating the new one, we have to generate a new child\_cert\_obj, so calling code that needs the updated child\_cert\_obj must use the return value from this method.

Definition at line 1172 of file rpki/rpkid.py.

**13.198.3.6 def rpki.rpkid.child\_cert\_obj.revoke ( self, publisher, generate\_crl\_and\_manifest = False )**

Revoke a child cert.

Definition at line 1156 of file rpki/rpkid.py.

#### 13.198.3.7 def rpki.rpkid.child\_cert\_obj.uri ( self )

Return the publication URI for this child\_cert.

Definition at line 1150 of file rpki/rpkid.py.

#### 13.198.3.8 def rpki.rpkid.child\_cert\_obj.uri\_tail ( self )

Return the tail (filename) portion of the URI for this child\_cert.

Definition at line 1143 of file rpki/rpkid.py.

### 13.198.4 Member Data Documentation

#### 13.198.4.1 rpki.rpkid.child\_cert\_obj.ca\_detail\_id

Definition at line 1117 of file rpki/rpkid.py.

#### 13.198.4.2 rpki.rpkid.child\_cert\_obj.cert

Definition at line 1117 of file rpki/rpkid.py.

#### 13.198.4.3 rpki.rpkid.child\_cert\_obj.child\_id

Definition at line 1117 of file rpki/rpkid.py.

#### 13.198.4.4 rpki.rpkid.child\_cert\_obj.gctx

Reimplemented from [rpki.sql.sql\\_persistent](#).

Definition at line 1117 of file `rpki/rpkid.py`.

#### 13.198.4.5 rpki.rpkid.child\_cert\_obj.published

Definition at line 1117 of file `rpki/rpkid.py`.

#### 13.198.4.6 tuple rpki.rpkid.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 1106 of file `rpki/rpkid.py`.

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

- [rpki/rpkid.py \(3793\)](#)

### 13.199 rpki.rpkid.ghostbuster\_obj Class Reference

Inheritance diagram for `rpki.rpkid.ghostbuster_obj`:

Collaboration diagram for `rpki.rpkid.ghostbuster_obj`:

#### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [ca\\_detail](#)
- def [generate](#)
- def [published\\_callback](#)
- def [regenerate](#)
- def [revoke](#)
- def [self](#)
- def [update](#)
- def [uri](#)

- def [uri\\_from\\_key](#)
- def [uri\\_tail](#)

#### Public Attributes

- [gctx](#)
- [self\\_id](#)

#### Static Public Attributes

- [ca\\_detail\\_id](#) = None
- [cert](#) = None
- [ghostbuster](#) = None
- [published](#) = None
- tuple [sql\\_template](#)
- [vcard](#) = None

#### 13.199.1 Detailed Description

Ghostbusters record.

Definition at line 1607 of file rpki/rpkid.py.

#### 13.199.2 Constructor & Destructor Documentation

**13.199.2.1** `def rpki.rpkid.ghostbuster_obj.__init__( self, gctx = None, self_id = None, ca_detail_id = None, vcard = None )`

Definition at line 1642 of file rpki/rpkid.py.

#### 13.199.3 Member Function Documentation

**13.199.3.1** `def rpki.rpkid.ghostbuster_obj.ca_detail( self )`

Fetch ca\_detail object to which this ghostbuster\_obj links.

Definition at line 1636 of file rpki/rpkid.py.

**13.199.3.2 def rpki.rpkid.ghostbuster\_obj.generate ( self, publisher, fast = False )**

Generate a Ghostbuster record

Once we have the right covering certificate, we generate the ghostbuster payload, generate a new EE certificate, use the EE certificate to sign the ghostbuster payload, publish the result, then throw away the private key for the EE cert. This is modeled after the way we handle ROAs.

If fast is set, we leave generating the new manifest for our caller to handle, presumably at the end of a bulk operation.

Definition at line 1667 of file rpki/rpkid.py.

**13.199.3.3 def rpki.rpkid.ghostbuster\_obj.published\_callback ( self, pdu )**

Check publication result.

Definition at line 1701 of file rpki/rpkid.py.

**13.199.3.4 def rpki.rpkid.ghostbuster\_obj.regenerate ( self, publisher, fast = False )**

Reissue Ghostbuster associated with this ghostbuster\_obj.

Definition at line 1744 of file rpki/rpkid.py.

**13.199.3.5 def rpki.rpkid.ghostbuster\_obj.revoke ( self, publisher, regenerate = False, allow\_failure = False, fast = False )**

Withdraw Ghostbuster associated with this ghostbuster\_obj.

In order to preserve make-before-break properties without duplicating code, this method also handles generating a replacement ghostbuster when requested.

If allow\_failure is set, failing to withdraw the ghostbuster will not be considered an error.

If fast is set, SQL actions will be deferred, on the assumption that our caller will handle regenerating CRL and manifest and flushing the SQL cache.

Definition at line 1709 of file rpki/rpkid.py.

#### 13.199.3.6 def rpki.rpkid.ghostbuster\_obj.self ( self )

Fetch self object to which this ghostbuster\_obj links.

Definition at line 1629 of file rpki/rpkid.py.

#### 13.199.3.7 def rpki.rpkid.ghostbuster\_obj.update ( self, publisher, fast = False )

Bring this ghostbuster\_obj up to date if necessary.

Definition at line 1652 of file rpki/rpkid.py.

#### 13.199.3.8 def rpki.rpkid.ghostbuster\_obj.uri ( self )

Return the publication URI for this ghostbuster\_obj's ghostbuster.

Definition at line 1760 of file rpki/rpkid.py.

#### 13.199.3.9 def rpki.rpkid.ghostbuster\_obj.uri\_from\_key ( self, key )

Return publication URI for a public key.

Definition at line 1753 of file rpki/rpkid.py.

#### 13.199.3.10 def rpki.rpkid.ghostbuster\_obj.uri\_tail ( self )



Return the tail (filename portion) of the publication URI for this ghostbuster\_obj's ghostbuster.

Definition at line 1767 of file rpki/rpkid.py.

#### 13.199.4 Member Data Documentation

##### 13.199.4.1 rpki.rpkid.ghostbuster\_obj.ca\_detail\_id = None [static]

Definition at line 1622 of file rpki/rpkid.py.

##### 13.199.4.2 rpki.rpkid.ghostbuster\_obj.cert = None [static]

Definition at line 1623 of file rpki/rpkid.py.

##### 13.199.4.3 rpki.rpkid.ghostbuster\_obj.getx

Reimplemented from [rpki.sql.sql\\_persistent](#).

Definition at line 1642 of file rpki/rpkid.py.

##### 13.199.4.4 rpki.rpkid.ghostbuster\_obj.ghostbuster = None [static]

Definition at line 1624 of file rpki/rpkid.py.

##### 13.199.4.5 rpki.rpkid.ghostbuster\_obj.published = None [static]

Definition at line 1625 of file rpki/rpkid.py.

##### 13.199.4.6 rpki.rpkid.ghostbuster\_obj.self\_id

Definition at line 1642 of file rpki/rpkid.py.

### 13.199.4.7 tuple rpki.rpkid.ghostbuster\_obj.sql\_template [static]

Initial value:

```
rpki.sql.template(
 "ghostbuster",
 "ghostbuster_id",
 "ca_detail_id",
 "self_id",
 "vcard",
 ("ghostbuster", rpki.x509.Ghostbuster),
 ("cert", rpki.x509.X509),
 ("published", rpki.sundial.datetime))
```

Definition at line 1612 of file rpki/rpkid.py.

### 13.199.4.8 rpki.rpkid.ghostbuster\_obj.vcard = None [static]

Definition at line 1626 of file rpki/rpkid.py.

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

- [rpki/rpkid.py \(3793\)](#)

## 13.200 rpki.rpkid.main Class Reference

Inheritance diagram for rpki.rpkid.main:

Collaboration diagram for rpki.rpkid.main:

### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [checkpoint](#)
- def [cron](#)
- def [cronjob\\_handler](#)
- def [irdb\\_query](#)
- def [irdb\\_query\\_child\\_resources](#)
- def [irdb\\_query\\_ghostbuster\\_requests](#)
- def [irdb\\_query\\_roa\\_requests](#)
- def [left\\_right\\_handler](#)
- def [main](#)
- def [start\\_cron](#)
- def [up\\_down\\_handler](#)

**Public Attributes**

- [bpki\\_ta](#)
- [cfg](#)
- [cfg\\_file](#)
- [cron\\_keepalive](#)
- [cron\\_period](#)
- [cron\\_timeout](#)
- [cron\\_timer](#)
- [http\\_server\\_host](#)
- [http\\_server\\_port](#)
- [initial\\_delay](#)
- [irbe\\_cert](#)
- [irdb\\_cert](#)
- [irdb\\_url](#)
- [profile](#)
- [publication\\_kludge\\_base](#)
- [rpkid\\_cert](#)
- [rpkid\\_key](#)
- [sql](#)
- [use\\_internal\\_cron](#)

**Static Public Attributes**

- tuple [up\\_down\\_url\\_regexp](#) = re.compile("/up-down/([-A-Z0-9\_]+)/([-A-Z0-9\_-]+)\$", re.I)

**13.200.1 Detailed Description**

Main program for rpkid.

Definition at line 43 of file rpki/rpkid.py.

**13.200.2 Constructor & Destructor Documentation****13.200.2.1 def rpki.rpkid.main.\_\_init\_\_ ( *self* )**

Definition at line 48 of file rpki/rpkid.py.

**13.200.2.2 def rpki.rpkid.main.main ( *self* )**

Definition at line 78 of file rpki/rpkid.py.

**13.200.3 Member Function Documentation****13.200.3.1 def rpki.rpkid.main.checkpoint ( *self* )**

Record that we were still alive when we got here, by resetting keepalive timer.

Definition at line 280 of file rpki/rpkid.py.

**13.200.3.2 def rpki.rpkid.main.cron ( *self*, *cb* = *None* )**

Periodic tasks.

Definition at line 288 of file rpki/rpkid.py.

**13.200.3.3 def rpki.rpkid.main.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 345 of file rpki/rpkid.py.

**13.200.3.4 def rpki.rpkid.main.irdb\_query ( *self*, *callback*, *errback*, *q\_pdup*, *kwargs* )**

Perform an IRDB callback query.

Definition at line 141 of file rpki/rpkid.py.

**13.200.3.5** `def rpki.rpkid.main.irdb_query_child_resources ( self,  
self_handle, child_handle, callback, errback )`

Ask IRDB about a child's resources.

Definition at line 174 of file rpki/rpkid.py.

**13.200.3.6** `def rpki.rpkid.main.irdb_query_ghostbuster_requests ( self,  
self_handle, parent_handles, callback, errback )`

Ask IRDB about self's ghostbuster record requests.

Definition at line 206 of file rpki/rpkid.py.

**13.200.3.7** `def rpki.rpkid.main.irdb_query_roa_requests ( self, self_handle,  
callback, errback )`

Ask IRDB about self's ROA requests.

Definition at line 194 of file rpki/rpkid.py.

**13.200.3.8** `def rpki.rpkid.main.left_right_handler ( self, query, path, cb )`

Process one left-right PDU.

Definition at line 223 of file rpki/rpkid.py.

**13.200.3.9** `def rpki.rpkid.main.start_cron ( self )`

Start clock for rpkid's internal cron process.

Definition at line 128 of file rpki/rpkid.py.

**13.200.3.10 def rpki.rpkid.main.up\_down\_handler ( *self*, *query*, *path*, *cb* )**

Process one up-down PDU.

Definition at line 249 of file rpki/rpkid.py.

**13.200.4 Member Data Documentation****13.200.4.1 rpki.rpkid.main.bpki\_ta**

Definition at line 78 of file rpki/rpkid.py.

**13.200.4.2 rpki.rpkid.main.cfg**

Definition at line 78 of file rpki/rpkid.py.

**13.200.4.3 rpki.rpkid.main.cfg\_file**

Definition at line 48 of file rpki/rpkid.py.

**13.200.4.4 rpki.rpkid.main.cron\_keepalive**

Definition at line 78 of file rpki/rpkid.py.

**13.200.4.5 rpki.rpkid.main.cron\_period**

Definition at line 78 of file rpki/rpkid.py.

**13.200.4.6 rpki.rpkid.main.cron\_timeout**

Definition at line 78 of file rpki/rpkid.py.

**13.200.4.7 rpki.rpkid.main.cron\_timer**

Definition at line 130 of file rpki/rpkid.py.

**13.200.4.8 rpki.rpkid.main.http\_server\_host**

Definition at line 78 of file rpki/rpkid.py.

**13.200.4.9 rpki.rpkid.main.http\_server\_port**

Definition at line 78 of file rpki/rpkid.py.

**13.200.4.10 rpki.rpkid.main.initial\_delay**

Definition at line 78 of file rpki/rpkid.py.

**13.200.4.11 rpki.rpkid.main.irbe\_cert**

Definition at line 78 of file rpki/rpkid.py.

**13.200.4.12 rpki.rpkid.main.irdb\_cert**

Definition at line 78 of file rpki/rpkid.py.

**13.200.4.13 rpki.rpkid.main.irdb\_url**

Definition at line 78 of file rpki/rpkid.py.

**13.200.4.14 rpki.rpkid.main.profile**

Definition at line 48 of file rpki/rpkid.py.

**13.200.4.15 rpki.rpkid.main.publication\_kludge\_base**

Definition at line 78 of file rpki/rpkid.py.

**13.200.4.16 rpki.rpkid.main.rpkid\_cert**

Definition at line 78 of file rpki/rpkid.py.

**13.200.4.17 rpki.rpkid.main.rpkid\_key**

Definition at line 78 of file rpki/rpkid.py.

**13.200.4.18 rpki.rpkid.main.sql**

Definition at line 78 of file rpki/rpkid.py.

**13.200.4.19** `tuple rpki.rpkid.main.up_down_url_regexp =  
re.compile("/up-down/([-A-Z0-9_]+)/([-A-Z0-9_]+)$", re.I)  
[static]`

Definition at line 247 of file rpki/rpkid.py.

**13.200.4.20 rpki.rpkid.main.use\_internal\_cron**

Definition at line 78 of file rpki/rpkid.py.

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



- [rpki/rpkid.py \(3793\)](#)

## 13.201 rpki.rpkid.publication\_queue Class Reference

Inheritance diagram for rpki.rpkid.publication\_queue:

Collaboration diagram for rpki.rpkid.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`

#### 13.201.1 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 1775 of file `rpki/rpkid.py`.

### 13.201.2 Constructor & Destructor Documentation

#### 13.201.2.1 def rpki.rpkid.publication\_queue.\_\_init\_\_ ( *self* )

Definition at line 1788 of file rpki/rpkid.py.

### 13.201.3 Member Function Documentation

#### 13.201.3.1 def rpki.rpkid.publication\_queue.add ( *self*, *uri*, *obj*, *repository*, *handler*, *make\_pdu* ) [private]

Definition at line 1795 of file rpki/rpkid.py.

#### 13.201.3.2 def rpki.rpkid.publication\_queue.call\_pubd ( *self*, *cb*, *eb* )

Definition at line 1817 of file rpki/rpkid.py.

#### 13.201.3.3 def rpki.rpkid.publication\_queue.publish ( *self*, *cls*, *uri*, *obj*, *repository*, *handler* = *None* )

Definition at line 1811 of file rpki/rpkid.py.

#### 13.201.3.4 def rpki.rpkid.publication\_queue.withdraw ( *self*, *cls*, *uri*, *obj*, *repository*, *handler* = *None* )

Definition at line 1814 of file rpki/rpkid.py.

### 13.201.4 Member Data Documentation

#### 13.201.4.1 rpki.rpkid.publication\_queue.handlers

Definition at line 1788 of file rpki/rpkid.py.

#### 13.201.4.2 rpki.rpkid.publication\_queue.msgs

Definition at line 1788 of file rpki/rpkid.py.

#### 13.201.4.3 rpki.rpkid.publication\_queue.replace = True [static]

Definition at line 1786 of file rpki/rpkid.py.

#### 13.201.4.4 rpki.rpkid.publication\_queue.repositories

Definition at line 1788 of file rpki/rpkid.py.

#### 13.201.4.5 rpki.rpkid.publication\_queue.uris

Definition at line 1788 of file rpki/rpkid.py.

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

- [rpki/rpkid.py \(3793\)](#)

### 13.202 rpki.rpkid.revoked\_cert\_obj Class Reference

Inheritance diagram for rpki.rpkid.revoked\_cert\_obj:

Collaboration diagram for rpki.rpkid.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](#)

#### 13.202.1 Detailed Description

Tombstone for a revoked certificate.

Definition at line 1294 of file rpki/rpkid.py.

#### 13.202.2 Constructor & Destructor Documentation

**13.202.2.1** `def rpki.rpkid.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 1307 of file rpki/rpkid.py.

#### 13.202.3 Member Function Documentation

**13.202.3.1** `def rpki.rpkid.revoked_cert_obj.ca_detail( self )`

Fetch `ca_detail` object to which this `revoked_cert_obj` links.

Definition at line 1321 of file rpki/rpkid.py.

**13.202.3.2** `def rpki.rpkid.revoked_cert_obj.revoke( cls, cert, ca_detail )`

Revoke a certificate.

Definition at line 1328 of file rpki/rpkid.py.

#### 13.202.4 Member Data Documentation

##### 13.202.4.1 rpki.rpkid.revoked\_cert\_obj.ca\_detail\_id

Definition at line 1309 of file rpki/rpkid.py.

##### 13.202.4.2 rpki.rpkid.revoked\_cert\_obj.expires

Definition at line 1309 of file rpki/rpkid.py.

##### 13.202.4.3 rpki.rpkid.revoked\_cert\_obj.gctx

Reimplemented from [rpki.sql.sql\\_persistent](#).

Definition at line 1309 of file rpki/rpkid.py.

##### 13.202.4.4 rpki.rpkid.revoked\_cert\_obj.revoked

Definition at line 1309 of file rpki/rpkid.py.

##### 13.202.4.5 rpki.rpkid.revoked\_cert\_obj.serial

Definition at line 1309 of file rpki/rpkid.py.

##### 13.202.4.6 tuple rpki.rpkid.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 1299 of file rpki/rpkid.py.

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

- [rpki/rpkid.py \(3793\)](#)

### 13.203 rpki.rpkid.roa\_obj Class Reference

Inheritance diagram for rpki.rpkid.roa\_obj:

Collaboration diagram for rpki.rpkid.roa\_obj:

#### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [\\_\\_repr\\_\\_](#)
- 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\\_from\\_key](#)
- 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`

#### 13.203.1 Detailed Description

Route Origin Authorization.

Definition at line 1339 of file `rpki/rpkid.py`.

#### 13.203.2 Constructor & Destructor Documentation

**13.203.2.1** `def rpki.rpkid.roa_obj.__init__( self, gctx = None, self_id = None, asn = None, ipv4 = None, ipv6 = None )`

Definition at line 1412 of file `rpki/rpkid.py`.

#### 13.203.3 Member Function Documentation

**13.203.3.1** `def rpki.rpkid.roa_obj.__repr__( self )`

Definition at line 1407 of file `rpki/rpkid.py`.

**13.203.3.2** `def rpki.rpkid.roa_obj.ca_detail( self )`

Fetch `ca_detail` object to which this `roa_obj` links.

Definition at line 1367 of file `rpki/rpkid.py`.

**13.203.3.3** `def rpki.rpkid.roa_obj.generate( self, publisher, fast = False )`

Generate a ROA.

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.

If fast is set, we leave generating the new manifest for our caller to handle, presumably at the end of a bulk operation.

Definition at line 1464 of file rpki/rpkid.py.

#### 13.203.3.4 def rpki.rpkid.roa\_obj.published\_callback ( self, pdu )

Check publication result.

Definition at line 1531 of file rpki/rpkid.py.

#### 13.203.3.5 def rpki.rpkid.roa\_obj.regenerate ( self, publisher, fast = False )

Reissue ROA associated with this roa\_obj.

Definition at line 1576 of file rpki/rpkid.py.

#### 13.203.3.6 def rpki.rpkid.roa\_obj.revoke ( self, publisher, regenerate = False, allow\_failure = False, fast = 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.



If fast is set, SQL actions will be deferred, on the assumption that our caller will handle regenerating CRL and manifest and flushing the SQL cache.

Definition at line 1539 of file rpki/rpkid.py.

### 13.203.3.7 def rpki.rpkid.roa\_obj.self ( self )

Fetch self object to which this roa\_obj links.

Definition at line 1360 of file rpki/rpkid.py.

### 13.203.3.8 def rpki.rpkid.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 1401 of file rpki/rpkid.py.

### 13.203.3.9 def rpki.rpkid.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 1373 of file rpki/rpkid.py.

### 13.203.3.10 def rpki.rpkid.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 1387 of file rpki/rpkid.py.

**13.203.3.11 def rpki.rpkid.roa\_obj.update ( self, publisher, fast = *False* )**

Bring this roa\_obj's ROA up to date if necessary.

Definition at line 1425 of file rpki/rpkid.py.

**13.203.3.12 def rpki.rpkid.roa\_obj.uri ( self )**

Return the publication URI for this roa\_obj's ROA.

Definition at line 1592 of file rpki/rpkid.py.

**13.203.3.13 def rpki.rpkid.roa\_obj.uri\_from\_key ( self, key )**

Return publication URI for a public key.

Definition at line 1585 of file rpki/rpkid.py.

**13.203.3.14 def rpki.rpkid.roa\_obj.uri\_tail ( self )**

Return the tail (filename portion) of the publication URI for this roa\_obj's ROA.

Definition at line 1599 of file rpki/rpkid.py.

**13.203.4 Member Data Documentation****13.203.4.1 rpki.rpkid.roa\_obj.asn**

Definition at line 1412 of file rpki/rpkid.py.

**13.203.4.2 rpki.rpkid.roa\_obj.ca\_detail\_id = None [static]**

Definition at line 1354 of file rpki/rpkid.py.

**13.203.4.3 rpki.rpkid.roa\_obj.cert = None [static]**

Definition at line 1355 of file rpki/rpkid.py.

**13.203.4.4 rpki.rpkid.roa\_obj.gctx**

Reimplemented from [rpki.sql.sql\\_persistent](#).

Definition at line 1412 of file rpki/rpkid.py.

**13.203.4.5 rpki.rpkid.roa\_obj.ipv4**

Definition at line 1412 of file rpki/rpkid.py.

**13.203.4.6 rpki.rpkid.roa\_obj.ipv6**

Definition at line 1412 of file rpki/rpkid.py.

**13.203.4.7 rpki.rpkid.roa\_obj.published = None [static]**

Definition at line 1357 of file rpki/rpkid.py.

**13.203.4.8 rpki.rpkid.roa\_obj.roa = None [static]**

Definition at line 1356 of file rpki/rpkid.py.

**13.203.4.9 rpki.rpkid.roa\_obj.self\_id**

Definition at line 1412 of file rpki/rpkid.py.

### 13.203.4.10 tuple rpki.rpkid.roa\_obj.sql\_template [static]

Initial value:

```
rpki.sql.template(
 "roa",
 "roa_id",
 "ca_detail_id",
 "self_id",
 "asn",
 ("roa", rpki.x509.ROA),
 ("cert", rpki.x509.X509),
 ("published", rpki.sundial.datetime))
```

Definition at line 1344 of file rpki/rpkid.py.

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

- [rpki/rpkid.py \(3793\)](#)

## 13.204 rpki.sql.session Class Reference

Inheritance diagram for rpki.sql.session:

Collaboration diagram for rpki.sql.session:

### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [assert\\_pristine](#)
- def [cache\\_clear](#)
- def [close](#)
- def [connect](#)
- def [execute](#)
- def [executemany](#)
- def [fetchall](#)
- def [lastrowid](#)
- def [ping](#)
- def [sweep](#)

### Public Attributes

- [cache](#)
- [cur](#)
- [database](#)

- [db](#)
- [dirty](#)
- [password](#)
- [username](#)

#### Private Member Functions

- [def \\_wrap\\_execute](#)

#### Static Private Attributes

- [\\_exceptions\\_enabled](#) = False

#### 13.204.1 Detailed Description

SQL session layer.

Definition at line 50 of file sql.py.

#### 13.204.2 Constructor & Destructor Documentation

##### 13.204.2.1 `def rpki.sql.session.__init__( self, cfg )`

Definition at line 57 of file sql.py.

#### 13.204.3 Member Function Documentation

##### 13.204.3.1 `def rpki.sql.session._wrap_execute( self, func, query, args )` `[private]`

Definition at line 88 of file sql.py.

##### 13.204.3.2 `def rpki.sql.session.assert_pristine( self )`

Assert that there are no dirty objects in the cache.

Definition at line 114 of file sql.py.

**13.204.3.3 def rpki.sql.session.cache\_clear ( self )**

Clear the object cache.

Definition at line 108 of file sql.py.

**13.204.3.4 def rpki.sql.session.close ( self )**

Definition at line 77 of file sql.py.

**13.204.3.5 def rpki.sql.session.connect ( self )**

Definition at line 72 of file sql.py.

**13.204.3.6 def rpki.sql.session.execute ( self, query, args = None )**

Definition at line 96 of file sql.py.

**13.204.3.7 def rpki.sql.session.executemany ( self, query, args )**

Definition at line 99 of file sql.py.

**13.204.3.8 def rpki.sql.session.fetchall ( self )**

Definition at line 102 of file sql.py.

**13.204.3.9 def rpki.sql.session.lastrowid ( self )**

Definition at line 105 of file sql.py.

**13.204.3.10 def rpki.sql.session.ping ( self )**

Definition at line 85 of file sql.py.

**13.204.3.11 def rpki.sql.session.sweep ( self )**

Write any dirty objects out to SQL.

Definition at line 120 of file sql.py.

**13.204.4 Member Data Documentation****13.204.4.1 rpki.sql.session.\_exceptions\_enabled = False [static, private]**

Definition at line 55 of file sql.py.

**13.204.4.2 rpki.sql.session.cache**

Definition at line 57 of file sql.py.

**13.204.4.3 rpki.sql.session.cur**

Definition at line 72 of file sql.py.

**13.204.4.4 rpki.sql.session.database**

Definition at line 57 of file sql.py.

**13.204.4.5 rpki.sql.session.db**

Definition at line 72 of file sql.py.

#### 13.204.4.6 rpki.sql.session.dirty

Definition at line 57 of file sql.py.

#### 13.204.4.7 rpki.sql.session.password

Definition at line 57 of file sql.py.

#### 13.204.4.8 rpki.sql.session.username

Definition at line 57 of file sql.py.

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

- [sql.py \(3551\)](#)

### 13.205 rpki.sql.sql\_persistent Class Reference

Inheritance diagram for rpki.sql.sql\_persistent:

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.*

#### 13.205.1 Detailed Description

Mixin for persistent class that needs to be stored in SQL.

Definition at line 158 of file sql.py.

#### 13.205.2 Member Function Documentation

##### 13.205.2.1 def rpki.sql.sql\_persistent.sql\_decode ( self, vals )

Initialize an object with values returned by `self.sql_fetch()`. This is a default version that assumes a one-to-one mapping between column names in SQL and attribute names in Python. If you need something fancier, override this.

Reimplemented in [rpki.rpkid.ca\\_detail\\_obj](#).

Definition at line 339 of file sql.py.

**13.205.2.2 def rpki.sql.sql\_persistent.sql\_delete ( self )**

Delete this object from SQL.

Definition at line 310 of file sql.py.

**13.205.2.3 def rpki.sql.sql\_persistent.sql\_delete\_hook ( self )**

Customization hook.

Reimplemented in [rpki.rpkid.roa\\_obj](#).

Definition at line 371 of file sql.py.

**13.205.2.4 def rpki.sql.sql\_persistent.sql\_encode ( self )**

Convert object attributes into a dict for use with canned SQL queries. This is a default version that assumes a one-to-one mapping between column names in SQL and attribute names in Python. If you need something fancier, override this.

Definition at line 326 of file sql.py.

**13.205.2.5 def rpki.sql.sql\_persistent.sql\_fetch ( cls, gctx, id )**

Fetch one object from SQL, based on its primary key.

Since in this one case we know that the primary index is also the cache key, we check for a cache hit directly in the hope of bypassing the SQL lookup entirely.

This method is usually called via a one-line class-specific wrapper. As a convenience, we also accept an id of None, and just return None in this case.

Definition at line 179 of file sql.py.

**13.205.2.6 def rpki.sql.sql\_persistent.sql\_fetch\_all ( cls, gctx )**

Fetch all objects of this type from SQL.

Definition at line 217 of file sql.py.

**13.205.2.7 def rpki.sql.sql\_persistent.sql\_fetch\_hook ( self )**

Customization hook.

Reimplemented in [rpki.rpkid.roa\\_obj](#).

Definition at line 352 of file sql.py.

**13.205.2.8 def rpki.sql.sql\_persistent.sql\_fetch\_where ( cls, gctx, where, args = None, also\_from = None )**

Fetch objects of this type matching an arbitrary SQL WHERE expression.

Definition at line 224 of file sql.py.

**13.205.2.9 def rpki.sql.sql\_persistent.sql\_fetch\_where1 ( cls, gctx, where, args = None, also\_from = None )**

Fetch one object from SQL, based on an arbitrary SQL WHERE expression.

Definition at line 202 of file sql.py.

**13.205.2.10 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 251 of file sql.py.

**13.205.2.11 def rpki.sql.sql\_persistent.sql\_insert\_hook ( *self* )**

Customization hook.

Reimplemented in [rpki.rpkid.roa\\_obj](#).

Definition at line 358 of file sql.py.

**13.205.2.12 def rpki.sql.sql\_persistent.sql\_is\_dirty ( *self* )**

Query whether this object needs to be written back to SQL.

Definition at line 275 of file sql.py.

**13.205.2.13 def rpki.sql.sql\_persistent.sql\_mark\_clean ( *self* )**

Mark this object as not needing to be written back to SQL.

Definition at line 269 of file sql.py.

**13.205.2.14 def rpki.sql.sql\_persistent.sql\_mark\_deleted ( *self* )**

Mark this object as needing to be deleted in SQL.

Definition at line 281 of file sql.py.

**13.205.2.15 def rpki.sql.sql\_persistent.sql\_mark\_dirty ( *self* )**

Mark this object as needing to be written back to SQL.

Definition at line 263 of file sql.py.

**13.205.2.16 def rpki.sql.sql\_persistent.sql\_store ( *self* )**

Store this object to SQL.

Definition at line 288 of file sql.py.

**13.205.2.17 def rpki.sql.sql\_persistent.sql\_update\_hook ( *self* )**

Customization hook.

Definition at line 364 of file sql.py.

**13.205.3 Member Data Documentation****13.205.3.1 rpki.sql.sql\_persistent.gctx**

Reimplemented in [rpki.rpkid.ca\\_obj](#), [rpki.rpkid.ca\\_detail\\_obj](#), [rpki.rpkid.child\\_cert\\_obj](#), [rpki.rpkid.revoked\\_cert\\_obj](#), [rpki.rpkid.roa\\_obj](#), and [rpki.rpkid.ghostbuster\\_obj](#).

Definition at line 253 of file sql.py.

**13.205.3.2 rpki::sql.sql\_persistent::sql\_debug = False [static]**

Enable logging of SQL actions.

Definition at line 176 of file sql.py.

**13.205.3.3 rpki::sql.sql\_persistent::sql\_deleted = False [static]**

Whether our cached copy of this object has been deleted.

Definition at line 171 of file sql.py.

**13.205.3.4 rpki::sql.sql\_persistent::sql\_in\_db = False [static]**

Whether this object is already in SQL or not.

Definition at line 166 of file sql.py.

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

- [sql.py \(3551\)](#)

## 13.206 rpki.sql.template Class Reference

Inheritance diagram for rpki.sql.template:

Collaboration diagram for rpki.sql.template:

### Public Member Functions

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

### Public Attributes

- [columns](#)
- [delete](#)
- [index](#)
- [insert](#)
- [map](#)
- [select](#)
- [table](#)
- [update](#)

### 13.206.1 Detailed Description

SQL template generator.

Definition at line 132 of file sql.py.

### 13.206.2 Constructor & Destructor Documentation

#### 13.206.2.1 `def rpki.sql.template.__init__( self, table_name, index_column, data_columns )`

Build a SQL template.

Definition at line 137 of file sql.py.

**13.206.3 Member Data Documentation****13.206.3.1 rpki.sql.template.columns**

Definition at line 139 of file sql.py.

**13.206.3.2 rpki.sql.template.delete**

Definition at line 139 of file sql.py.

**13.206.3.3 rpki.sql.template.index**

Definition at line 139 of file sql.py.

**13.206.3.4 rpki.sql.template.insert**

Definition at line 139 of file sql.py.

**13.206.3.5 rpki.sql.template.map**

Definition at line 139 of file sql.py.

**13.206.3.6 rpki.sql.template.select**

Definition at line 139 of file sql.py.

**13.206.3.7 rpki.sql.template.table**

Definition at line 139 of file sql.py.

### 13.206.3.8 rpki.sql.template.update

Definition at line 139 of file sql.py.

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

- [sql.py \(3551\)](#)

## 13.207 rpki.sundial.datetime Class Reference

Inheritance diagram for rpki.sundial.datetime:

Collaboration diagram for rpki.sundial.datetime:

### Public Member Functions

- def [\\_\\_add\\_\\_](#)
- def [\\_\\_radd\\_\\_](#)
- def [\\_\\_rsub\\_\\_](#)
- def [\\_\\_str\\_\\_](#)
- def [\\_\\_sub\\_\\_](#)
- def [earlier](#)
- def [from\\_sql](#)
- def [fromASN1tuple](#)
- def [fromdatetime](#)
- def [fromGeneralizedTime](#)
- def [fromOpenSSL](#)
- 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.*



### 13.207.1 Detailed Description

RPKI extensions to standard `datetime.datetime` class. All work here is in UTC, so we use naive `datetime` objects.

Definition at line 56 of file `sundial.py`.

### 13.207.2 Member Function Documentation

#### 13.207.2.1 `def rpki.sundial.datetime.__add__( self, y )`

Definition at line 192 of file `sundial.py`.

#### 13.207.2.2 `def rpki.sundial.datetime.__radd__( self, y )`

Definition at line 193 of file `sundial.py`.

#### 13.207.2.3 `def rpki.sundial.datetime.__rsub__( self, y )`

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

#### 13.207.2.4 `def rpki.sundial.datetime.__str__( self )`

Definition at line 137 of file `sundial.py`.

#### 13.207.2.5 `def rpki.sundial.datetime.__sub__( self, y )`

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

#### 13.207.2.6 `def rpki.sundial.datetime.earlier( self, other )`

Return the earlier of two timestamps.

Definition at line 186 of file sundial.py.

#### 13.207.2.7 def rpki.sundial.datetime.from\_sql ( cls, x )

Convert from SQL storage format.

Definition at line 159 of file sundial.py.

#### 13.207.2.8 def rpki.sundial.datetime.fromASN1tuple ( cls, x )

Convert from ASN.1 tuple representation.

Definition at line 97 of file sundial.py.

#### 13.207.2.9 def rpki.sundial.datetime.fromdatetime ( cls, x )

Convert a datetime.datetime object into this subclass. This is whacky due to the weird constructors for datetime.

Definition at line 141 of file sundial.py.

#### 13.207.2.10 def rpki.sundial.datetime.fromGeneralizedTime ( cls, x )

Convert from ASN.1 GeneralizedTime.

Definition at line 84 of file sundial.py.

#### 13.207.2.11 def rpki.sundial.datetime.fromOpenSSL ( cls, x )

Convert from the format OpenSSL's command line tool uses into this subclass. May require rewriting if we run into locale problems.

Definition at line 149 of file sundial.py.

**13.207.2.12 def rpki.sundial.datetime.fromUTCTime ( cls, x )**

Convert from ASN.1 UTCTime.

Definition at line 70 of file sundial.py.

**13.207.2.13 def rpki.sundial.datetime.fromXMLtime ( cls, x )**

Convert from XML time representation.

Definition at line 122 of file sundial.py.

**13.207.2.14 def rpki.sundial.datetime.later ( self, other )**

Return the later of two timestamps.

Definition at line 180 of file sundial.py.

**13.207.2.15 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 165 of file sundial.py.

**13.207.2.16 def rpki.sundial.datetime.toASN1tuple ( self )**

Convert to ASN.1 tuple representation.

Definition at line 112 of file sundial.py.

**13.207.2.17 def rpki.sundial.datetime.toGeneralizedTime ( self )**

Convert to ASN.1 GeneralizedTime.

Definition at line 90 of file sundial.py.

**13.207.2.18 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 62 of file sundial.py.

**13.207.2.19 def rpki.sundial.datetime.toUTCTime ( self )**

Convert to ASN.1 UTCTime.

Definition at line 77 of file sundial.py.

**13.207.2.20 def rpki.sundial.datetime.toXMLtime ( self )**

Convert to XML time representation.

Definition at line 131 of file sundial.py.

**13.207.3 Member Data Documentation****13.207.3.1 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 110 of file sundial.py.

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

- [sundial.py \(3783\)](#)

## 13.208 rpki.sundial.timedelta Class Reference

Inheritance diagram for rpki.sundial.timedelta:

Collaboration diagram for rpki.sundial.timedelta:

### Public Member Functions

- def [\\_\\_abs\\_\\_](#)
- def [\\_\\_add\\_\\_](#)
- def [\\_\\_div\\_\\_](#)
- def [\\_\\_floordiv\\_\\_](#)
- def [\\_\\_mul\\_\\_](#)
- def [\\_\\_neg\\_\\_](#)
- def [\\_\\_pos\\_\\_](#)
- def [\\_\\_radd\\_\\_](#)
- def [\\_\\_rdiv\\_\\_](#)
- def [\\_\\_rfloordiv\\_\\_](#)
- def [\\_\\_rmul\\_\\_](#)
- def [\\_\\_rsub\\_\\_](#)
- def [\\_\\_sub\\_\\_](#)
- def [convert\\_to\\_seconds](#)
- def [fromtimedelta](#)
- def [parse](#)

### Static Public Attributes

- tuple [regex](#)  
*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).*

### 13.208.1 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 197 of file sundial.py.

### 13.208.2 Member Function Documentation

#### 13.208.2.1 def rpki.sundial.timedelta.\_\_abs\_\_( self )

Definition at line 276 of file sundial.py.

#### 13.208.2.2 def rpki.sundial.timedelta.\_\_add\_\_( self, x )

Definition at line 277 of file sundial.py.

#### 13.208.2.3 def rpki.sundial.timedelta.\_\_div\_\_( self, x )

Definition at line 278 of file sundial.py.

#### 13.208.2.4 def rpki.sundial.timedelta.\_\_floordiv\_\_( self, x )

Definition at line 279 of file sundial.py.

#### 13.208.2.5 def rpki.sundial.timedelta.\_\_mul\_\_( self, x )

Definition at line 280 of file sundial.py.

**13.208.2.6 def rpki.sundial.timedelta.\_\_neg\_\_ ( *self* )**

Definition at line 281 of file sundial.py.

**13.208.2.7 def rpki.sundial.timedelta.\_\_pos\_\_ ( *self* )**

Definition at line 282 of file sundial.py.

**13.208.2.8 def rpki.sundial.timedelta.\_\_radd\_\_ ( *self*, *x* )**

Definition at line 283 of file sundial.py.

**13.208.2.9 def rpki.sundial.timedelta.\_\_rdiv\_\_ ( *self*, *x* )**

Definition at line 284 of file sundial.py.

**13.208.2.10 def rpki.sundial.timedelta.\_\_rfloordiv\_\_ ( *self*, *x* )**

Definition at line 285 of file sundial.py.

**13.208.2.11 def rpki.sundial.timedelta.\_\_rmul\_\_ ( *self*, *x* )**

Definition at line 286 of file sundial.py.

**13.208.2.12 def rpki.sundial.timedelta.\_\_rsub\_\_ ( *self*, *x* )**

Definition at line 287 of file sundial.py.

**13.208.2.13 def rpki.sundial.timedelta.\_\_sub\_\_( self, x )**

Definition at line 288 of file sundial.py.

**13.208.2.14 def rpki.sundial.timedelta.convert\_to\_seconds( self )**

Convert a timedelta interval to seconds.

Definition at line 263 of file sundial.py.

**13.208.2.15 def rpki.sundial.timedelta.fromtimedelta( cls, x )**

Convert a datetime.timedelta object into this subclass.

Definition at line 270 of file sundial.py.

**13.208.2.16 def rpki.sundial.timedelta.parse( cls, arg )**

Parse text into a timedelta object.

Definition at line 242 of file sundial.py.

**13.208.3 Member Data Documentation****13.208.3.1 rpki::sundial.timedelta::regex [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 225 of file `sundial.py`.

### 13.208.3.2 rpki::sundial.timedelta::years\_to\_seconds = 31556926 [static]

Conversion factor from years to seconds (value furnished by the "units" program).

Definition at line 239 of file `sundial.py`.

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

- [sundial.py \(3783\)](#)

## 13.209 rpki.up\_down.base\_elt Class Reference

Inheritance diagram for `rpki.up_down.base_elt`:

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](#)

### 13.209.1 Detailed Description

Generic PDU object.

Virtual class, just provides some default methods.

Definition at line 43 of file `up_down.py`.

### 13.209.2 Member Function Documentation

#### 13.209.2.1 def rpki.up\_down.base\_elt.check\_response ( self )

Placeholder for response checking.

Reimplemented in [rpki.up\\_down.issue\\_response\\_pdu](#), and [rpki.up\\_down.error\\_response\\_pdu](#).

Definition at line 91 of file up\_down.py.

### 13.209.2.2 def rpki.up\_down.base\_elt.endElement ( self, stack, name, text )

Ignore endElement() if there's no specific handler.

If we don't need to do anything else, just pop the stack.

Reimplemented in [rpki.up\\_down.certificate\\_elt](#), [rpki.up\\_down.class\\_elt](#), [rpki.up\\_down.issue\\_pdu](#), and [rpki.up\\_down.error\\_response\\_pdu](#).

Definition at line 59 of file up\_down.py.

### 13.209.2.3 def rpki.up\_down.base\_elt.make\_b64elt ( self, elt, name, value )

Construct a sub-element with Base64 text content.

Definition at line 78 of file up\_down.py.

### 13.209.2.4 def rpki.up\_down.base\_elt.make\_elt ( self, name, attrs )

Construct a element, copying over a set of attributes.

Definition at line 67 of file up\_down.py.

### 13.209.2.5 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.rootd.list\\_pdu](#), [rpki.rootd.issue\\_pdu](#), [rpki.rootd.revoke\\_pdu](#), [rpki.up\\_down.list\\_pdu](#), [rpki.up\\_down.issue\\_pdu](#), and [rpki.up\\_down.revoke\\_pdu](#).

Definition at line 85 of file up\_down.py.

### 13.209.2.6 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 \(3746\)](#)

## 13.210 rpki.up\_down.certificate\_elt Class Reference

Inheritance diagram for rpki.up\_down.certificate\_elt:

Collaboration diagram for rpki.up\_down.certificate\_elt:

### Public Member Functions

- def [endElement](#)
- def [startElement](#)
- def [toXML](#)

### Public Attributes

- [cert](#)
- [cert\\_url](#)
- [req\\_resource\\_set\\_as](#)
- [req\\_resource\\_set\\_ipv4](#)
- [req\\_resource\\_set\\_ipv6](#)

### 13.210.1 Detailed Description

Up-Down protocol representation of an issued certificate.

Definition at line 132 of file up\_down.py.

### 13.210.2 Member Function Documentation

#### 13.210.2.1 `def rpki.up_down.certificate_elt.endElement ( self, stack, name, text )`

Handle text content of a <certificate/> element.

Reimplemented from [rpki.up\\_down.base\\_elt](#).

Definition at line 147 of file up\_down.py.

#### 13.210.2.2 `def rpki.up_down.certificate_elt.startElement ( self, stack, name, attrs )`

Handle attributes of <certificate/> element.

Reimplemented from [rpki.up\\_down.base\\_elt](#).

Definition at line 137 of file up\_down.py.

#### 13.210.2.3 `def rpki.up_down.certificate_elt.toXML ( self )`

Generate a <certificate/> element.

Definition at line 155 of file up\_down.py.

### 13.210.3 Member Data Documentation

#### 13.210.3.1 `rpki.up_down.certificate_elt.cert`

Definition at line 149 of file up\_down.py.

#### 13.210.3.2 `rpki.up_down.certificate_elt.cert_url`

Definition at line 139 of file up\_down.py.

### 13.210.3.3 rpki.up\_down.certificate\_elt.req\_resource\_set\_as

Definition at line 139 of file up\_down.py.

### 13.210.3.4 rpki.up\_down.certificate\_elt.req\_resource\_set\_ipv4

Definition at line 139 of file up\_down.py.

### 13.210.3.5 rpki.up\_down.certificate\_elt.req\_resource\_set\_ipv6

Definition at line 139 of file up\_down.py.

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

- [up\\_down.py \(3746\)](#)

## 13.211 rpki.up\_down.class\_elt Class Reference

Inheritance diagram for rpki.up\_down.class\_elt:

Collaboration diagram for rpki.up\_down.class\_elt:

### Public Member Functions

- [def \\_\\_init\\_\\_](#)
- [def endElement](#)
- [def from\\_resource\\_bag](#)
- [def startElement](#)
- [def to\\_resource\\_bag](#)
- [def toXML](#)

### Public Attributes

- [cert\\_url](#)
- [certs](#)
- [class\\_name](#)
- [resource\\_set\\_as](#)
- [resource\\_set\\_ipv4](#)

- [resource\\_set\\_ipv6](#)
- [resource\\_set\\_notafter](#)
- [suggested\\_sia\\_head](#)

#### Static Public Attributes

- [issuer](#) = None

#### 13.211.1 Detailed Description

Up-Down protocol representation of a resource class.

Definition at line 164 of file up\_down.py.

#### 13.211.2 Constructor & Destructor Documentation

##### 13.211.2.1 def rpki.up\_down.class\_elt.\_\_init\_\_( self )

Initialize class\_elt.

Definition at line 171 of file up\_down.py.

#### 13.211.3 Member Function Documentation

##### 13.211.3.1 def rpki.up\_down.class\_elt.endElement( self, stack, name, text )

Handle <class/> elements and their children.

Reimplemented from [rpki.up\\_down.base\\_elt](#).

Definition at line 197 of file up\_down.py.

##### 13.211.3.2 def rpki.up\_down.class\_elt.from\_resource\_bag( self, bag )

Set resources of this class element from a resource\_bag.

Definition at line 227 of file up\_down.py.

### 13.211.3.3 `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 178 of file up\_down.py.

### 13.211.3.4 `def rpki.up_down.class_elt.to_resource_bag ( self )`

Build a resource\_bag from from this <class/> element.

Definition at line 218 of file up\_down.py.

### 13.211.3.5 `def rpki.up_down.class_elt.toXML ( self )`

Generate a <class/> element.

Definition at line 207 of file up\_down.py.

## 13.211.4 Member Data Documentation

### 13.211.4.1 `rpki.up_down.class_elt.cert_url`

Definition at line 180 of file up\_down.py.

### 13.211.4.2 `rpki.up_down.class_elt.certs`

Definition at line 173 of file up\_down.py.

### 13.211.4.3 `rpki.up_down.class_elt.class_name`

Definition at line 180 of file up\_down.py.

**13.211.4.4 rpki.up\_down.class\_elt.issuer = None [static]**

Definition at line 169 of file up\_down.py.

**13.211.4.5 rpki.up\_down.class\_elt.resource\_set\_as**

Definition at line 180 of file up\_down.py.

**13.211.4.6 rpki.up\_down.class\_elt.resource\_set\_ipv4**

Definition at line 180 of file up\_down.py.

**13.211.4.7 rpki.up\_down.class\_elt.resource\_set\_ipv6**

Definition at line 180 of file up\_down.py.

**13.211.4.8 rpki.up\_down.class\_elt.resource\_set\_notafter**

Definition at line 180 of file up\_down.py.

**13.211.4.9 rpki.up\_down.class\_elt.suggested\_sia\_head**

Definition at line 180 of file up\_down.py.

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

- [up\\_down.py \(3746\)](#)

**13.212 rpki.up\_down.class\_response\_syntax Class Reference**

Inheritance diagram for rpki.up\_down.class\_response\_syntax:

Collaboration diagram for rpki.up\_down.class\_response\_syntax:



### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [startElement](#)
- def [toXML](#)

### Public Attributes

- [classes](#)

#### 13.212.1 Detailed Description

Syntax for Up-Down protocol "list\_response" and "issue\_response" PDUs.

Definition at line 292 of file up\_down.py.

#### 13.212.2 Constructor & Destructor Documentation

##### 13.212.2.1 def rpki.up\_down.class\_response\_syntax.\_\_init\_\_( self )

Initialize class\_response\_syntax.

Definition at line 297 of file up\_down.py.

#### 13.212.3 Member Function Documentation

##### 13.212.3.1 def rpki.up\_down.class\_response\_syntax.startElement( self, stack, name, attrs )

Handle "list\_response" and "issue\_response" PDUs.

Reimplemented from [rpki.up\\_down.base\\_elt](#).

Definition at line 304 of file up\_down.py.

##### 13.212.3.2 def rpki.up\_down.class\_response\_syntax.toXML( self )

Generate payload of "list\_response" and "issue\_response" PDUs.

Definition at line 314 of file up\_down.py.

#### 13.212.4 Member Data Documentation

##### 13.212.4.1 rpki.up\_down.class\_response\_syntax.classes

Definition at line 299 of file up\_down.py.

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

- [up\\_down.py \(3746\)](#)

#### 13.213 rpki.up\_down.cms\_msg Class Reference

Inheritance diagram for rpki.up\_down.cms\_msg:

Collaboration diagram for rpki.up\_down.cms\_msg:

##### Static Public Attributes

- string [encoding](#) = "UTF-8"
- [saxify](#) = sax\_handler.saxify
- [schema](#) = [rpki.relaxng.up\\_down](#)

##### 13.213.1 Detailed Description

Class to hold a CMS-signed up-down PDU.

Definition at line 699 of file up\_down.py.

##### 13.213.2 Member Data Documentation

###### 13.213.2.1 string rpki.up\_down.cms\_msg.encoding = "UTF-8" [static]

Definition at line 704 of file up\_down.py.

###### 13.213.2.2 rpki.up\_down.cms\_msg.saxify = sax\_handler.saxify [static]

Reimplemented in [rpki.rootd.cms\\_msg](#).

Definition at line 706 of file up\_down.py.

### 13.213.2.3 rpki.up\_down.cms\_msg.schema = rpki.relaxng.up\_down[static]

Definition at line 705 of file up\_down.py.

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

- [up\\_down.py \(3746\)](#)

## 13.214 rpki.up\_down.error\_response\_pdu Class Reference

Inheritance diagram for rpki.up\_down.error\_response\_pdu:

Collaboration diagram for rpki.up\_down.error\_response\_pdu:

### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [check\\_response](#)
- def [endElement](#)
- def [toXML](#)

### Public Attributes

- [description](#)
- [status](#)

### Static Public Attributes

- dictionary [codes](#)
- dictionary [exceptions](#)

#### 13.214.1 Detailed Description

Up-Down protocol "error\_response" PDU.

Definition at line 517 of file up\_down.py.

### 13.214.2 Constructor & Destructor Documentation

#### 13.214.2.1 `def rpki.up_down.error_response_pdu.__init__( self, exception = None )`

Initialize an `error_response` PDU from an exception object.

Definition at line 536 of file `up_down.py`.

### 13.214.3 Member Function Documentation

#### 13.214.3.1 `def rpki.up_down.error_response_pdu.check_response( self )`

Handle an error response. For now, just raise an exception, perhaps figure out something more clever to do later.

Reimplemented from [rpki.up\\_down.base\\_elt](#).

Definition at line 576 of file `up_down.py`.

#### 13.214.3.2 `def rpki.up_down.error_response_pdu.endElement( self, stack, name, text )`

Handle "error\_response" PDU.

Reimplemented from [rpki.up\\_down.base\\_elt](#).

Definition at line 545 of file `up_down.py`.

#### 13.214.3.3 `def rpki.up_down.error_response_pdu.toXML( self )`

Generate payload of "error\_response" PDU.

Definition at line 561 of file `up_down.py`.

#### 13.214.4 Member Data Documentation

##### 13.214.4.1 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 522 of file up\_down.py.

##### 13.214.4.2 rpki.up\_down.error\_response\_pdu.description

Definition at line 538 of file up\_down.py.

##### 13.214.4.3 dictionary rpki.up\_down.error\_response\_pdu.exceptions [static]

**Initial value:**

```
{
 rpki.exceptions.NoActiveCA : 1202 }
```

Definition at line 533 of file up\_down.py.

##### 13.214.4.4 rpki.up\_down.error\_response\_pdu.status

Definition at line 538 of file up\_down.py.

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

- [up\\_down.py \(3746\)](#)

## 13.215 rpki.up\_down.issue\_pdu Class Reference

Inheritance diagram for rpki.up\_down.issue\_pdu:

Collaboration diagram for rpki.up\_down.issue\_pdu:

### Public Member Functions

- def [endElement](#)
- def [query](#)
- def [serve\\_pdu](#)
- def [startElement](#)
- def [toXML](#)

### Public Attributes

- [class\\_name](#)
- [pkcs10](#)
- [req\\_resource\\_set\\_as](#)
- [req\\_resource\\_set\\_ipv4](#)
- [req\\_resource\\_set\\_ipv6](#)

### 13.215.1 Detailed Description

Up-Down protocol "issue" PDU.

Definition at line 324 of file up\_down.py.

### 13.215.2 Member Function Documentation

#### 13.215.2.1 def rpki.up\_down.issue\_pdu.endElement ( *self*, *stack*, *name*, *text* )

Handle "issue" PDU.

Reimplemented from [rpki.up\\_down.base\\_elt](#).

Definition at line 339 of file up\_down.py.

**13.215.2.2** `def rpki.up_down.issue_pdu.query ( cls, parent, ca, ca_detail, callback, errback )`

Send an "issue" request to parent associated with ca.

Definition at line 428 of file up\_down.py.

**13.215.2.3** `def rpki.up_down.issue_pdu.serve_pdu ( self, q_msg, r_msg, child, callback, errback )`

Serve one issue request PDU.

Reimplemented from [rpki.up\\_down.base\\_elt](#).

Reimplemented in [rpki.rootd.issue\\_pdu](#).

Definition at line 356 of file up\_down.py.

**13.215.2.4** `def rpki.up_down.issue_pdu.startElement ( self, stack, name, attrs )`

Handle "issue" PDU.

Reimplemented from [rpki.up\\_down.base\\_elt](#).

Definition at line 329 of file up\_down.py.

**13.215.2.5** `def rpki.up_down.issue_pdu.toXML ( self )`

Generate payload of "issue" PDU.

Definition at line 347 of file up\_down.py.

**13.215.3 Member Data Documentation****13.215.3.1** `rpki.up_down.issue_pdu.class_name`

Definition at line 331 of file up\_down.py.

### 13.215.3.2 rpki.up\_down.issue\_pdu.pkcs10

Definition at line 341 of file up\_down.py.

### 13.215.3.3 rpki.up\_down.issue\_pdu.req\_resource\_set\_as

Definition at line 331 of file up\_down.py.

### 13.215.3.4 rpki.up\_down.issue\_pdu.req\_resource\_set\_ipv4

Definition at line 331 of file up\_down.py.

### 13.215.3.5 rpki.up\_down.issue\_pdu.req\_resource\_set\_ipv6

Definition at line 331 of file up\_down.py.

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

- [up\\_down.py \(3746\)](#)

## 13.216 rpki.up\_down.issue\_response\_pdu Class Reference

Inheritance diagram for rpki.up\_down.issue\_response\_pdu:

Collaboration diagram for rpki.up\_down.issue\_response\_pdu:

### Public Member Functions

- def [check\\_response](#)

### 13.216.1 Detailed Description

Up-Down protocol "issue\_response" PDU.

Definition at line 441 of file up\_down.py.



### 13.216.2 Member Function Documentation

#### 13.216.2.1 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 446 of file up\_down.py.

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

- [up\\_down.py \(3746\)](#)

### 13.217 rpki.up\_down.list\_pdu Class Reference

Inheritance diagram for rpki.up\_down.list\_pdu:

Collaboration diagram for rpki.up\_down.list\_pdu:

#### Public Member Functions

- def [query](#)
- def [serve\\_pdu](#)
- def [toXML](#)

#### 13.217.1 Detailed Description

Up-Down protocol "list" PDU.

Definition at line 236 of file up\_down.py.

### 13.217.2 Member Function Documentation

#### 13.217.2.1 def rpki.up\_down.list\_pdu.query ( *cls*, *parent*, *cb*, *eb* )

Send a "list" query to parent.

Definition at line 280 of file up\_down.py.

### 13.217.2.2 `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 [rpki.rootd.list\\_pdu](#).

Definition at line 245 of file `up_down.py`.

### 13.217.2.3 `def rpki.up_down.list_pdu.toXML ( self )`

Generate (empty) payload of "list" PDU.

Definition at line 241 of file `up_down.py`.

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

- [up\\_down.py \(3746\)](#)

## 13.218 rpki.up\_down.list\_response\_pdu Class Reference

Inheritance diagram for `rpki.up_down.list_response_pdu`:

Collaboration diagram for `rpki.up_down.list_response_pdu`:

### 13.218.1 Detailed Description

Up-Down protocol "list\_response" PDU.

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

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

- [up\\_down.py \(3746\)](#)

## 13.219 rpki.up\_down.message\_pdu Class Reference

Inheritance diagram for `rpki.up_down.message_pdu`:

Collaboration diagram for `rpki.up_down.message_pdu`:

### Public Member Functions

- def [\\_\\_str\\_\\_](#)
- def [log\\_query](#)
- def [make\\_query](#)
- def [serve\\_error](#)
- def [serve\\_top\\_level](#)
- def [startElement](#)
- def [toXML](#)

### Public Attributes

- [payload](#)
- [recipient](#)
- [sender](#)
- [type](#)
- [version](#)

### Static Public Attributes

- dictionary [name2type](#)
- tuple [type2name](#) = [dict](#)((v, k) for k, v in [name2type](#).items())
- int [version](#) = 1

#### 13.219.1 Detailed Description

Up-Down protocol message wrapper PDU.

Definition at line 583 of file up\_down.py.

#### 13.219.2 Member Function Documentation

##### 13.219.2.1 def rpki.up\_down.message\_pdu.\_\_str\_\_ ( *self* )

Convert a message PDU to a string.

Definition at line 625 of file up\_down.py.

**13.219.2.2** `def rpki.up_down.message_pdu.log_query ( self, child )`

Log query we're handling. Separate method so rootd can override.

Reimplemented in [rpki.rootd.message\\_pdu](#).

Definition at line 656 of file up\_down.py.

**13.219.2.3** `def rpki.up_down.message_pdu.make_query ( cls, payload, sender, recipient )`

Construct one message PDU.

Definition at line 674 of file up\_down.py.

**13.219.2.4** `def rpki.up_down.message_pdu.serve_error ( self, exception )`

Generate an error\_response message PDU.

Definition at line 662 of file up\_down.py.

**13.219.2.5** `def rpki.up_down.message_pdu.serve_top_level ( self, child, callback )`

Serve one message request PDU.

Definition at line 631 of file up\_down.py.

**13.219.2.6** `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 609 of file up\_down.py.

### 13.219.2.7 def rpki.up\_down.message\_pdu.toXML ( self )

Generate payload of message PDU.

Definition at line 601 of file up\_down.py.

## 13.219.3 Member Data Documentation

### 13.219.3.1 dictionary rpki.up\_down.message\_pdu.name2type [static]

Initial value:

```
{
 "list" : list_pdu,
 "list_response" : list_response_pdu,
 "issue" : issue_pdu,
 "issue_response" : issue_response_pdu,
 "revoke" : revoke_pdu,
 "revoke_response": revoke_response_pdu,
 "error_response" : error_response_pdu }
```

Reimplemented in [rpki.rootd.message\\_pdu](#).

Definition at line 590 of file up\_down.py.

### 13.219.3.2 rpki.up\_down.message\_pdu.payload

Definition at line 615 of file up\_down.py.

### 13.219.3.3 rpki.up\_down.message\_pdu.recipient

Definition at line 615 of file up\_down.py.

### 13.219.3.4 rpki.up\_down.message\_pdu.sender

Definition at line 615 of file up\_down.py.

### 13.219.3.5 rpki.up\_down.message\_pdu.type

Definition at line 615 of file up\_down.py.

**13.219.3.6** tuple rpki.up\_down.message\_pdu.type2name = dict((v, k) for k, v in name2type.items()) **[static]**

Reimplemented in [rpki.rootd.message\\_pdu](#).

Definition at line 599 of file up\_down.py.

**13.219.3.7** int rpki.up\_down.message\_pdu.version = 1 **[static]**

Definition at line 588 of file up\_down.py.

### 13.219.3.8 rpki.up\_down.message\_pdu.version

Definition at line 615 of file up\_down.py.

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

- [up\\_down.py \(3746\)](#)

## 13.220 rpki.up\_down.multi\_uri Class Reference

Inheritance diagram for rpki.up\_down.multi\_uri:

Collaboration diagram for rpki.up\_down.multi\_uri:

### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [\\_\\_str\\_\\_](#)
- def [rsync](#)

### 13.220.1 Detailed Description

Container for a set of URIs.

Definition at line 97 of file up\_down.py.

### 13.220.2 Constructor & Destructor Documentation

#### 13.220.2.1 def rpki.up\_down.multi\_uri.\_\_init\_\_( self, ini )

Initialize a set of URIs, which includes basic some syntax checking.

Definition at line 102 of file up\_down.py.

### 13.220.3 Member Function Documentation

#### 13.220.3.1 def rpki.up\_down.multi\_uri.\_\_str\_\_( self )

Convert a multi\_uri back to a string representation.

Definition at line 117 of file up\_down.py.

#### 13.220.3.2 def rpki.up\_down.multi\_uri.rsync( self )

Find first rsync://... URI in self.

Definition at line 123 of file up\_down.py.

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

- [up\\_down.py \(3746\)](#)

## 13.221 rpki.up\_down.revoke\_pdu Class Reference

Inheritance diagram for rpki.up\_down.revoke\_pdu:

Collaboration diagram for rpki.up\_down.revoke\_pdu:

### Public Member Functions

- def [get\\_SKI](#)
- def [query](#)
- def [serve\\_pdu](#)

### Public Attributes

- [class\\_name](#)
- [ski](#)

#### 13.221.1 Detailed Description

Up-Down protocol "revoke" PDU.

Definition at line 468 of file up\_down.py.

#### 13.221.2 Member Function Documentation

##### 13.221.2.1 def rpki.up\_down.revoke\_pdu.get\_SKI ( *self* )

Convert *g*(SKI) encoding from PDU back to raw SKI.

Definition at line 473 of file up\_down.py.

##### 13.221.2.2 def rpki.up\_down.revoke\_pdu.query ( *cls*, *ca*, *gski*, *cb*, *eb* )

Send a "revoke" request for certificate(s) named by *gski* to parent associated with *ca*.

Definition at line 499 of file up\_down.py.

##### 13.221.2.3 def rpki.up\_down.revoke\_pdu.serve\_pdu ( *self*, *q\_msg*, *r\_msg*, *child*, *cb*, *eb* )

Serve one revoke request PDU.



Reimplemented from [rpki.up\\_down.base\\_elt](#).

Reimplemented in [rpki.rootd.revoke\\_pdu](#).

Definition at line 479 of file up\_down.py.

### 13.221.3 Member Data Documentation

#### 13.221.3.1 rpki.up\_down.revoke\_pdu.class\_name

Reimplemented from [rpki.up\\_down.revoke\\_syntax](#).

Definition at line 501 of file up\_down.py.

#### 13.221.3.2 rpki.up\_down.revoke\_pdu.ski

Reimplemented from [rpki.up\\_down.revoke\\_syntax](#).

Definition at line 501 of file up\_down.py.

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

- [up\\_down.py \(3746\)](#)

### 13.222 rpki.up\_down.revoke\_response\_pdu Class Reference

Inheritance diagram for rpki.up\_down.revoke\_response\_pdu:

Collaboration diagram for rpki.up\_down.revoke\_response\_pdu:

#### 13.222.1 Detailed Description

Up-Down protocol "revoke\_response" PDU.

Definition at line 510 of file up\_down.py.

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

- [up\\_down.py \(3746\)](#)

### 13.223 rpki.up\_down.revoke\_syntax Class Reference

Inheritance diagram for rpki.up\_down.revoke\_syntax:

Collaboration diagram for rpki.up\_down.revoke\_syntax:

#### Public Member Functions

- def [startElement](#)
- def [toXML](#)

#### Public Attributes

- [class\\_name](#)
- [ski](#)

#### 13.223.1 Detailed Description

Syntax for Up-Down protocol "revoke" and "revoke\_response" PDUs.

Definition at line 454 of file up\_down.py.

#### 13.223.2 Member Function Documentation

##### 13.223.2.1 def rpki.up\_down.revoke\_syntax.startElement ( *self*, *stack*, *name*, *attrs* )

Handle "revoke" PDU.

Reimplemented from [rpki.up\\_down.base\\_elt](#).

Definition at line 459 of file up\_down.py.

##### 13.223.2.2 def rpki.up\_down.revoke\_syntax.toXML ( *self* )

Generate payload of "revoke" PDU.

Definition at line 464 of file up\_down.py.

### 13.223.3 Member Data Documentation

#### 13.223.3.1 `rpki.up_down.revoke_syntax.class_name`

Reimplemented in [rpki.up\\_down.revoke\\_pdu](#).

Definition at line 459 of file `up_down.py`.

#### 13.223.3.2 `rpki.up_down.revoke_syntax.ski`

Reimplemented in [rpki.up\\_down.revoke\\_pdu](#).

Definition at line 459 of file `up_down.py`.

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

- [up\\_down.py](#) (3746)

## 13.224 `rpki.up_down.sax_handler` Class Reference

Inheritance diagram for `rpki.up_down.sax_handler`:

Collaboration diagram for `rpki.up_down.sax_handler`:

### Static Public Attributes

- string `name` = "message"
- `pdu` = `message_pdu`
- string `version` = "1"

#### 13.224.1 Detailed Description

SAX handler for Up-Down protocol.

Definition at line 690 of file `up_down.py`.

#### 13.224.2 Member Data Documentation

##### 13.224.2.1 string `rpki.up_down.sax_handler.name` = "message" `[static]`

Definition at line 696 of file up\_down.py.

#### 13.224.2.2 rpki.up\_down.sax\_handler.pdu = message\_pdu [static]

Reimplemented in [rpki.rootd.sax\\_handler](#).

Definition at line 695 of file up\_down.py.

#### 13.224.2.3 string rpki.up\_down.sax\_handler.version = "1" [static]

Definition at line 697 of file up\_down.py.

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

- [up\\_down.py \(3746\)](#)

### 13.225 rpki.x509.CMS\_object Class Reference

Inheritance diagram for rpki.x509.CMS\_object:

Collaboration diagram for rpki.x509.CMS\_object:

#### Public Member Functions

- def [extract](#)
- def [get\\_content](#)
- def [get\\_DER](#)
- def [get\\_POW](#)
- def [get\\_signingTime](#)
- 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.*

**13.225.1 Detailed Description**

Class to hold a CMS-wrapped object.

CMS-wrapped objects are a little different from the other DER\_object types because the signed object is CMS wrapping inner content that's also ASN.1, and due to our current minimal support for CMS we can't just handle this as a pretty composite object. So, for now anyway, a CMS\_object is the outer CMS wrapped object so that the usual DER and PEM operations do the obvious things, and the inner content is handle via separate methods.

Definition at line 809 of file x509.py.

**13.225.2 Member Function Documentation****13.225.2.1 def rpki.x509.CMS\_object.extract ( self )**

Extract and store inner content from CMS wrapper without verifying the CMS.

DANGER WILL ROBINSON!!!

Do not use this method on unvalidated data. Use the `verify()` method instead.

If you don't understand this warning, don't use this method.

Definition at line 966 of file `x509.py`.

#### 13.225.2.2 `def rpki.x509.CMS_object.get_content ( self )`

Get the inner content of this `CMS_object`.

Definition at line 871 of file `x509.py`.

#### 13.225.2.3 `def rpki.x509.CMS_object.get_DER ( self )`

Get the DER value of this `CMS_object`.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 850 of file `x509.py`.

#### 13.225.2.4 `def rpki.x509.CMS_object.get_POW ( self )`

Get the `rpki.POW` value of this `CMS_object`.

Definition at line 862 of file `x509.py`.

#### 13.225.2.5 `def rpki.x509.CMS_object.get_signingTime ( self )`

Extract `signingTime` from CMS signed attributes.

Definition at line 886 of file `x509.py`.

**13.225.2.6 def rpki.x509.CMS\_object.set\_content ( self, content )**

Set the (inner) content of this CMS\_object, clearing the wrapper.

Definition at line 879 of file x509.py.

**13.225.2.7 def rpki.x509.CMS\_object.sign ( self, keypair, certs, crls = None, no\_certs = False )**

Sign and wrap inner content.

Definition at line 994 of file x509.py.

**13.225.2.8 def rpki.x509.CMS\_object.verify ( self, ta )**

Verify CMS wrapper and store inner content.

Definition at line 892 of file x509.py.

**13.225.3 Member Data Documentation****13.225.3.1 rpki.x509.CMS\_object.content**

Reimplemented in [rpki.x509.DER\\_CMS\\_object](#), [rpki.x509.XML\\_CMS\\_object](#), and [rpki.x509.Ghostbuster](#).

Definition at line 881 of file x509.py.

**13.225.3.2 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 835 of file x509.py.

### 13.225.3.3 rpki.x509.CMS\_object.DER

DER value of this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 852 of file x509.py.

### 13.225.3.4 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 830 of file x509.py.

### 13.225.3.5 tuple rpki.x509.CMS\_object.econtent\_oid = POWify\_OID("id-data") [static]

Reimplemented in [rpki.x509.SignedManifest](#), [rpki.x509.ROA](#), [rpki.x509.XML\\_CMS\\_object](#), and [rpki.x509.Ghostbuster](#).

Definition at line 824 of file x509.py.

### 13.225.3.6 tuple rpki.x509.CMS\_object.formats = ("DER", "POW") [static]

Formats supported in this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 822 of file x509.py.

### 13.225.3.7 tuple rpki.x509.CMS\_object.other\_clear = ("content",) [static]

Other attributes that self.clear() should whack.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 823 of file x509.py.



**13.225.3.8** `tuple rpki.x509.CMS_object.pem_converter =  
PEM_converter("CMS") [static]`

PEM converter for this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Reimplemented in [rpki.x509.SignedManifest](#), [rpki.x509.ROA](#), and [rpki.x509.Ghostbuster](#).

Definition at line 825 of file x509.py.

**13.225.3.9** `rpki.x509.CMS_object.POW`

Definition at line 864 of file x509.py.

**13.225.3.10** `rpki::x509.CMS_object::print_on_der_error = True [static]`

Set this to True to log alleged DER when we have trouble parsing it, in case it's really a Perl backtrace or something.

Definition at line 848 of file x509.py.

**13.225.3.11** `rpki::x509.CMS_object::require_crls = False [static]`

Set this to False to make CMS CRLs optional in the cases where we would otherwise require them.

Some day this option should go away and CRLs should be unconditionally mandatory in such cases.

Definition at line 842 of file x509.py.

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

- [x509.py \(3793\)](#)

**13.226** `rpki.x509.CRL Class Reference`

Inheritance diagram for `rpki.x509.CRL`:

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.*

#### 13.226.1 Detailed Description

Class to hold a Certificate Revocation List.

Definition at line 1258 of file x509.py.

#### 13.226.2 Member Function Documentation

**13.226.2.1** `def rpki.x509.CRL.generate ( cls, keypair, issuer, serial, thisUpdate, nextUpdate, revokedCertificates, version = 1, digestType = "sha256WithRSAEncryption" )`

Generate a new CRL.

Definition at line 1320 of file x509.py.

**13.226.2.2 def rpki.x509.CRL.get\_DER ( self )**

Get the DER value of this CRL.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 1266 of file x509.py.

**13.226.2.3 def rpki.x509.CRL.get\_POW ( self )**

Get the rpki.POW value of this CRL.

Definition at line 1281 of file x509.py.

**13.226.2.4 def rpki.x509.CRL.get\_POWpkix ( self )**

Get the rpki.POW.pkix value of this CRL.

Definition at line 1290 of file x509.py.

**13.226.2.5 def rpki.x509.CRL.getIssuer ( self )**

Get issuer value of this CRL.

Definition at line 1313 of file x509.py.

**13.226.2.6 def rpki.x509.CRL.getNextUpdate ( self )**

Get nextUpdate value from this CRL.

Definition at line 1307 of file x509.py.

### 13.226.2.7 def rpki.x509.CRL.getThisUpdate ( self )

Get thisUpdate value from this CRL.

Definition at line 1301 of file x509.py.

## 13.226.3 Member Data Documentation

### 13.226.3.1 rpki.x509.CRL.DER

DER value of this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 1268 of file x509.py.

### 13.226.3.2 tuple rpki.x509.CRL.formats = ("DER", "POW", "POWpkix") [static]

Formats supported in this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 1263 of file x509.py.

### 13.226.3.3 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 1264 of file x509.py.

### 13.226.3.4 rpki.x509.CRL.POW

Definition at line 1283 of file x509.py.

### 13.226.3.5 rpki.x509.CRL.POWpkix

Definition at line 1292 of file x509.py.

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

- [x509.py \(3793\)](#)

### 13.227 rpki.x509.DeadDrop Class Reference

Inheritance diagram for rpki.x509.DeadDrop:

Collaboration diagram for rpki.x509.DeadDrop:

#### Public Member Functions

- def [\\_\\_init\\_\\_](#)
- def [dump](#)

#### Public Attributes

- [maildir](#)
- [pid](#)

#### 13.227.1 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 1121 of file x509.py.

#### 13.227.2 Constructor & Destructor Documentation

##### 13.227.2.1 def rpki.x509.DeadDrop.\_\_init\_\_( self, name )

Definition at line 1129 of file x509.py.

### 13.227.3 Member Function Documentation

#### 13.227.3.1 def rpki.x509.DeadDrop.dump ( *self*, *obj* )

Definition at line 1133 of file x509.py.

### 13.227.4 Member Data Documentation

#### 13.227.4.1 rpki.x509.DeadDrop.maildir

Definition at line 1129 of file x509.py.

#### 13.227.4.2 rpki.x509.DeadDrop.pid

Definition at line 1129 of file x509.py.

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

- [x509.py \(3793\)](#)

## 13.228 rpki.x509.DER\_CMS\_object Class Reference

Inheritance diagram for rpki.x509.DER\_CMS\_object:

Collaboration diagram for rpki.x509.DER\_CMS\_object:

### Public Member Functions

- def [decode](#)
- def [encode](#)

### Public Attributes

- [content](#)

#### 13.228.1 Detailed Description

Class to hold CMS objects with DER-based content.

Definition at line 1030 of file x509.py.

### 13.228.2 Member Function Documentation

#### 13.228.2.1 def rpki.x509.DER\_CMS\_object.decode ( self, der )

Decode DER and set inner content.

Definition at line 1041 of file x509.py.

#### 13.228.2.2 def rpki.x509.DER\_CMS\_object.encode ( self )

Encode inner content for signing.

Definition at line 1035 of file x509.py.

### 13.228.3 Member Data Documentation

#### 13.228.3.1 rpki.x509.DER\_CMS\_object.content

Reimplemented from [rpki.x509.CMS\\_object](#).

Definition at line 1043 of file x509.py.

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

- [x509.py \(3793\)](#)

## 13.229 rpki.x509.DER\_object Class Reference

Inheritance diagram for rpki.x509.DER\_object:

Collaboration diagram for rpki.x509.DER\_object:

### Public Member Functions

- [def \\_\\_cmp\\_\\_](#)
- [def \\_\\_init\\_\\_](#)

- def [check](#)
- def [check\\_auto\\_update](#)
- 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.*
- [filename](#)
- [timestamp](#)

#### 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.*

### 13.229.1 Detailed Description

Virtual class to hold a generic DER object.

Definition at line 121 of file x509.py.

### 13.229.2 Constructor & Destructor Documentation

#### 13.229.2.1 `def rpki.x509.DER_object.__init__( self, kw )`

Initialize a DER\_object.

Definition at line 153 of file x509.py.

### 13.229.3 Member Function Documentation

#### 13.229.3.1 `def rpki.x509.DER_object.__cmp__( self, other )`

Compare two DER-encoded objects.

Definition at line 250 of file x509.py.

#### 13.229.3.2 `def rpki.x509.DER_object.check( self )`

Perform basic checks on a DER object.

Definition at line 220 of file x509.py.

#### 13.229.3.3 `def rpki.x509.DER_object.check_auto_update( self )`

Check for updates to a DER object that auto-updates from a file.

Definition at line 200 of file x509.py.

**13.229.3.4 def rpki.x509.DER\_object.clear ( self )**

Make this object empty.

Definition at line 144 of file x509.py.

**13.229.3.5 def rpki.x509.DER\_object.dumpasn1 ( self )**

Pretty print an ASN.1 DER object using cryptlib dumpasn1 tool.  
Use a temporary file rather than popen4() because dumpasn1 uses  
seek() when decoding ASN.1 content nested in OCTET STRING values.

Definition at line 383 of file x509.py.

**13.229.3.6 def rpki.x509.DER\_object.empty ( self )**

Test whether this object is empty.

Definition at line 138 of file x509.py.

**13.229.3.7 def rpki.x509.DER\_object.from\_sql ( cls, x )**

Convert from SQL storage format.

Definition at line 371 of file x509.py.

**13.229.3.8 def rpki.x509.DER\_object.gAKI ( self )**

Calculate g(AKI) for this object. Only work for subclasses  
that implement get\_AKI().

Definition at line 286 of file x509.py.

**13.229.3.9 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 358 of file x509.py.

**13.229.3.10 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 329 of file x509.py.

**13.229.3.11 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 336 of file x509.py.

**13.229.3.12 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 293 of file x509.py.

**13.229.3.13 def rpki.x509.DER\_object.get\_Base64 ( self )**

Get the Base64 encoding of the DER value of this object.

Definition at line 238 of file x509.py.

**13.229.3.14 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 343 of file x509.py.

**13.229.3.15 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 227 of file x509.py.

**13.229.3.16 def rpki.x509.DER\_object.get\_PEM ( self )**

Get the PEM representation of this object.

Definition at line 244 of file x509.py.

**13.229.3.17 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 308 of file x509.py.

**13.229.3.18 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 315 of file x509.py.

**13.229.3.19 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 322 of file x509.py.

**13.229.3.20 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 301 of file x509.py.

**13.229.3.21 def rpki.x509.DER\_object.gSKI ( self )**

Calculate g(SKI) for this object. Only work for subclasses  
that implement get\_SKI().

Definition at line 271 of file x509.py.

**13.229.3.22 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 278 of file x509.py.

**13.229.3.23 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 263 of file x509.py.

**13.229.3.24 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 350 of file x509.py.

**13.229.3.25 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 161 of file x509.py.

**13.229.3.26 def rpki.x509.DER\_object.to\_sql ( self )**

Convert to SQL storage format.

Definition at line 377 of file x509.py.

**13.229.4 Member Data Documentation****13.229.4.1 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 168 of file x509.py.

**13.229.4.2 rpki.x509.DER\_object.filename**

Definition at line 146 of file x509.py.

**13.229.4.3 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 127 of file x509.py.

**13.229.4.4 tuple rpki.x509.DER\_object.other\_clear = () [static]**

Other attributes that self.clear() should whack.

Reimplemented in [rpki.x509.CMS\\_object](#).

Definition at line 133 of file x509.py.

**13.229.4.5 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](#), [rpki.x509.Ghostbuster](#), and [rpki.x509.CRL](#).

Definition at line 130 of file x509.py.

**13.229.4.6 rpki.x509.DER\_object.timestamp**

Definition at line 146 of file x509.py.

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

- [x509.py \(3793\)](#)

**13.230 rpki.x509.Ghostbuster Class Reference**

Inheritance diagram for rpki.x509.Ghostbuster:

Collaboration diagram for rpki.x509.Ghostbuster:

### Public Member Functions

- def [build](#)
- def [decode](#)
- def [encode](#)

### Public Attributes

- [content](#)

### Static Public Attributes

- tuple [econtent\\_oid](#) = POWify\_OID("id-ct-rpkiGhostbusters")
- tuple [pem\\_converter](#) = [PEM\\_converter](#)("GHOSTBUSTERS RECORD")  
*PEM converter for this object.*

#### 13.230.1 Detailed Description

Class to hold Ghostbusters record (CMS-wrapped VCard). This is quite minimal because we treat the VCard as an opaque byte string managed by the back-end.

Definition at line 1223 of file x509.py.

#### 13.230.2 Member Function Documentation

##### 13.230.2.1 def rpki.x509.Ghostbuster.build ( cls, vcard, keypair, certs )

Build a Ghostbuster record.

Definition at line 1248 of file x509.py.

##### 13.230.2.2 def rpki.x509.Ghostbuster.decode ( self, vcard )

Decode XML and set inner content. At the moment we're treating the VCard as an opaque byte string, so no encoding needed here.

Definition at line 1240 of file x509.py.



### 13.230.2.3 def rpki.x509.Ghostbuster.encode ( self )

Encode inner content for signing. At the moment we're treating the VCard as an opaque byte string, so no encoding needed here.

Definition at line 1233 of file x509.py.

## 13.230.3 Member Data Documentation

### 13.230.3.1 rpki.x509.Ghostbuster.content

Reimplemented from [rpki.x509.CMS\\_object](#).

Definition at line 1243 of file x509.py.

### 13.230.3.2 tuple rpki.x509.Ghostbuster.econtent\_oid = POWify\_OID("id-ct-rpkiGhostbusters") [static]

Reimplemented from [rpki.x509.CMS\\_object](#).

Definition at line 1231 of file x509.py.

### 13.230.3.3 tuple rpki.x509.Ghostbuster.pem\_converter = PEM\_converter("GHOSTBUSTERS RECORD") [static]

PEM converter for this object.

Reimplemented from [rpki.x509.CMS\\_object](#).

Definition at line 1230 of file x509.py.

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

- [x509.py \(3793\)](#)

## 13.231 rpki.x509.PEM\_converter Class Reference

Inheritance diagram for rpki.x509.PEM\_converter:

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`

#### 13.231.1 Detailed Description

Convert between DER and PEM encodings for various kinds of ASN.1 data.

Definition at line 71 of file x509.py.

#### 13.231.2 Constructor & Destructor Documentation

##### 13.231.2.1 `def rpki.x509.PEM_converter.__init__( self, kind )`

Initialize PEM\_converter.

Definition at line 76 of file x509.py.

#### 13.231.3 Member Function Documentation

##### 13.231.3.1 `def rpki.x509.PEM_converter.looks_like_PEM( self, text )`

Guess whether text looks like a PEM encoding.

Definition at line 83 of file x509.py.

##### 13.231.3.2 `def rpki.x509.PEM_converter.to_DER( self, pem )`

Convert from PEM to DER.

Definition at line 90 of file x509.py.

### 13.231.3.3 def rpki.x509.PEM\_converter.to\_PEM ( self, der )

Convert from DER to PEM.

Definition at line 103 of file x509.py.

#### 13.231.4 Member Data Documentation

##### 13.231.4.1 rpki.x509.PEM\_converter.b

Definition at line 78 of file x509.py.

##### 13.231.4.2 rpki.x509.PEM\_converter.e

Definition at line 78 of file x509.py.

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

- [x509.py \(3793\)](#)

### 13.232 rpki.x509.PKCS10 Class Reference

Inheritance diagram for rpki.x509.PKCS10:

Collaboration diagram for rpki.x509.PKCS10:

#### Public Member Functions

- def [check\\_valid\\_rpki](#)
- def [create](#)
- def [create\\_ca](#)
- def [get\\_DER](#)
- def [get\\_POWpkix](#)
- def [getPublicKey](#)

### Public Attributes

- [DER](#)  
*DER value of this object.*
- [POWpkix](#)

### Static Public Attributes

- tuple `formats` = ("DER", "[POWpkix](#)")  
*Formats supported in this object.*
- tuple `pem_converter` = [PEM\\_converter](#)("CERTIFICATE REQUEST")  
*PEM converter for this object.*

#### 13.232.1 Detailed Description

Class to hold a PKCS #10 request.

Definition at line 598 of file x509.py.

#### 13.232.2 Member Function Documentation

##### 13.232.2.1 `def rpki.x509.PKCS10.check_valid_rpki ( self )`

Check this certification request to see whether it's a valid request for an RPKI certificate. This is broken out of the up-down protocol code because it's somewhat involved and the up-down code doesn't need to know the details.

Throws an exception if the request isn't valid, so if this method returns at all, the request is ok.

Definition at line 635 of file x509.py.

##### 13.232.2.2 `def rpki.x509.PKCS10.create ( cls, keypair, exts = None )`

Create a new request for a given keypair, including given extensions.

Definition at line 695 of file x509.py.

**13.232.2.3 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 682 of file x509.py.

**13.232.2.4 def rpki.x509.PKCS10.get\_DER ( self )**

Get the DER value of this certification request.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 606 of file x509.py.

**13.232.2.5 def rpki.x509.PKCS10.get\_POWpkix ( self )**

Get the rpki.POW.pkix value of this certification request.

Definition at line 618 of file x509.py.

**13.232.2.6 def rpki.x509.PKCS10.getPublicKey ( self )**

Extract the public key from this certification request.

Definition at line 629 of file x509.py.

**13.232.3 Member Data Documentation****13.232.3.1 rpki.x509.PKCS10.DER**

DER value of this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 608 of file x509.py.

**13.232.3.2** `tuple rpki.x509.PKCS10.formats = ("DER", "POWpkix")`  
`[static]`

Formats supported in this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 603 of file x509.py.

**13.232.3.3** `tuple rpki.x509.PKCS10.pem_converter =`  
`PEM_converter("CERTIFICATE REQUEST") [static]`

PEM converter for this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 604 of file x509.py.

**13.232.3.4** `rpki.x509.PKCS10.POWpkix`

Definition at line 620 of file x509.py.

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

- [x509.py \(3793\)](#)

**13.233 rpki.x509.ROA Class Reference**

Inheritance diagram for rpki.x509.ROA:

Collaboration diagram for rpki.x509.ROA:

#### Public Member Functions

- def [build](#)

#### Static Public Attributes

- `content_class` = [rpki.roa.RouteOriginAttestation](#)
- tuple `econtent_oid` = `POWify_OID("id-ct-routeOriginAttestation")`
- tuple `pem_converter` = `PEM_converter("ROUTE ORIGIN ATTESTATION")`

*PEM converter for this object.*

### 13.233.1 Detailed Description

Class to hold a signed ROA.

Definition at line 1093 of file x509.py.

### 13.233.2 Member Function Documentation

#### 13.233.2.1 `def rpki.x509.ROA.build ( cls, asn, ipv4, ipv6, keypair, certs, version = 0 )`

Build a ROA.

Definition at line 1103 of file x509.py.

### 13.233.3 Member Data Documentation

#### 13.233.3.1 `rpki.x509.ROA.content_class = rpki.roa.RouteOriginAttestation [static]`

Definition at line 1099 of file x509.py.

#### 13.233.3.2 `tuple rpki.x509.ROA.econtent_oid = POWify_OID("id-ct-routeOriginAttestation") [static]`

Reimplemented from [rpki.x509.CMS\\_object](#).

Definition at line 1100 of file x509.py.

#### 13.233.3.3 `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 1098 of file x509.py.

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

- [x509.py \(3793\)](#)

## 13.234 rpki.x509.RSA Class Reference

Inheritance diagram for rpki.x509.RSA:

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.*

#### 13.234.1 Detailed Description

Class to hold an RSA key pair.

Definition at line 709 of file x509.py.



### 13.234.2 Member Function Documentation

#### 13.234.2.1 `def rpki.x509.RSA.generate ( cls, keylength = 2048 )`

Generate a new keypair.

Definition at line 739 of file x509.py.

#### 13.234.2.2 `def rpki.x509.RSA.get_DER ( self )`

Get the DER value of this keypair.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 717 of file x509.py.

#### 13.234.2.3 `def rpki.x509.RSA.get_POW ( self )`

Get the rpki.POW value of this keypair.

Definition at line 729 of file x509.py.

#### 13.234.2.4 `def rpki.x509.RSA.get_public_DER ( self )`

Get the DER encoding of the public key from this keypair.

Definition at line 746 of file x509.py.

#### 13.234.2.5 `def rpki.x509.RSA.get_RSAPublic ( self )`

Convert the public key of this keypair into a RSAPublic object.

Definition at line 758 of file x509.py.

**13.234.2.6 def rpki.x509.RSA.get\_SKI ( self )**

Calculate the SKI of this keypair.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 752 of file x509.py.

**13.234.3 Member Data Documentation****13.234.3.1 rpki.x509.RSA.DER**

DER value of this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 719 of file x509.py.

**13.234.3.2 tuple rpki.x509.RSA.formats = ("DER", "POW") [static]**

Formats supported in this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 714 of file x509.py.

**13.234.3.3 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 715 of file x509.py.

**13.234.3.4 rpki.x509.RSA.POW**

Definition at line 731 of file x509.py.

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

- [x509.py \(3793\)](#)

### 13.235 rpki.x509.RSAPublic Class Reference

Inheritance diagram for rpki.x509.RSAPublic:

Collaboration diagram for rpki.x509.RSAPublic:

#### Public Member Functions

- def [get\\_DER](#)
- def [get\\_POW](#)
- def [get\\_SKI](#)

#### Public Attributes

- [DER](#)  
*DER value of this object.*
- [POW](#)

#### Static Public Attributes

- tuple [formats](#) = ("DER", "[POW](#)")  
*Formats supported in this object.*
- tuple [pem\\_converter](#) = [PEM\\_converter](#)("RSA PUBLIC KEY")  
*PEM converter for this object.*

#### 13.235.1 Detailed Description

Class to hold an RSA public key.

Definition at line 764 of file x509.py.

#### 13.235.2 Member Function Documentation

##### 13.235.2.1 def rpki.x509.RSAPublic.get\_DER ( self )

Get the DER value of this public key.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 772 of file x509.py.

### 13.235.2.2 def rpki.x509.RSAPublic.get\_POW ( self )

Get the rpki.POW value of this public key.

Definition at line 784 of file x509.py.

### 13.235.2.3 def rpki.x509.RSAPublic.get\_SKI ( self )

Calculate the SKI of this public key.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 793 of file x509.py.

## 13.235.3 Member Data Documentation

### 13.235.3.1 rpki.x509.RSAPublic.DER

DER value of this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 774 of file x509.py.

### 13.235.3.2 tuple rpki.x509.RSAPublic.formats = ("DER", "POW") [static]

Formats supported in this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 769 of file x509.py.

### 13.235.3.3 tuple rpki.x509.RSAPublic.pem\_converter = PEM\_converter("RSA PUBLIC KEY") [static]

PEM converter for this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 770 of file x509.py.

### 13.235.3.4 rpki.x509.RSAPublic.POW

Definition at line 786 of file x509.py.

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

- [x509.py \(3793\)](#)

## 13.236 rpki.x509.SignedManifest Class Reference

Inheritance diagram for rpki.x509.SignedManifest:

Collaboration diagram for rpki.x509.SignedManifest:

### Public Member Functions

- def [build](#)
- def [getNextUpdate](#)
- def [getThisUpdate](#)

### Static Public Attributes

- [content\\_class](#) = [rpki.manifest.Manifest](#)
- tuple [econtent\\_oid](#) = POWify\_OID("id-ct-rpkiManifest")
- tuple [pem\\_converter](#) = [PEM\\_converter](#)("RPKI MANIFEST")

*PEM converter for this object.*

### 13.236.1 Detailed Description

Class to hold a signed manifest.

Definition at line 1049 of file x509.py.

### 13.236.2 Member Function Documentation

**13.236.2.1** `def rpki.x509.SignedManifest.build ( cls, serial, thisUpdate, nextUpdate, names_and_objs, keypair, certs, version = 0 )`

Build a signed manifest.

Definition at line 1071 of file x509.py.

**13.236.2.2** `def rpki.x509.SignedManifest.getNextUpdate ( self )`

Get nextUpdate value from this manifest.

Definition at line 1064 of file x509.py.

**13.236.2.3** `def rpki.x509.SignedManifest.getThisUpdate ( self )`

Get thisUpdate value from this manifest.

Definition at line 1058 of file x509.py.

### 13.236.3 Member Data Documentation

**13.236.3.1** `rpki.x509.SignedManifest.content_class = rpki.manifest.Manifest [static]`

Definition at line 1055 of file x509.py.

**13.236.3.2** `tuple rpki.x509.SignedManifest.econtent_oid = POWify_OID("id-ct-rpkiManifest") [static]`

Reimplemented from [rpki.x509.CMS\\_object](#).

Definition at line 1056 of file x509.py.

**13.236.3.3** tuple rpki.x509.SignedManifest.pem\_converter =  
PEM\_converter("RPKI MANIFEST") [static]

PEM converter for this object.

Reimplemented from [rpki.x509.CMS\\_object](#).

Definition at line 1054 of file x509.py.

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

- [x509.py \(3793\)](#)

## 13.237 rpki.x509.X509 Class Reference

Inheritance diagram for rpki.x509.X509:

Collaboration diagram for rpki.x509.X509:

### Public Member Functions

- def [cross\\_certify](#)
- def [expired](#)
- def [get\\_DER](#)
- def [get\\_POW](#)
- def [get\\_POWpkix](#)
- def [getIssuer](#)
- def [getNotAfter](#)
- def [getNotBefore](#)
- def [getPublicKey](#)
- def [getSerial](#)
- def [getSubject](#)
- def [issue](#)
- def [normalize\\_chain](#)

### Public Attributes

- [DER](#)  
*DER value of this object.*
- [POW](#)
- [POWpkix](#)

### Static Public Attributes

- tuple `formats` = ("DER", "POW", "POWpkix")  
*Formats supported in this object.*
- tuple `pem_converter` = `PEM_converter`("CERTIFICATE")  
*PEM converter for this object.*

### 13.237.1 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 404 of file x509.py.

### 13.237.2 Member Function Documentation

#### 13.237.2.1 `def rpki.x509.X509.cross_certify ( self, keypair, source_cert, serial, notAfter, now = None, pathLenConstraint = 0 )`

Issue a certificate with values taking from an existing certificate. This is used to construct some kinds of BPKI certificates.

Definition at line 556 of file x509.py.

#### 13.237.2.2 `def rpki.x509.X509.expired ( self )`

Test whether this certificate has expired.

Definition at line 489 of file x509.py.

#### 13.237.2.3 `def rpki.x509.X509.get_DER ( self )`



Get the DER value of this certificate.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 418 of file x509.py.

#### 13.237.2.4 def rpki.x509.X509.get\_POW ( self )

Get the rpki.POW value of this certificate.

Definition at line 433 of file x509.py.

#### 13.237.2.5 def rpki.x509.X509.get\_POWpkix ( self )

Get the rpki.POW.pkix value of this certificate.

Definition at line 442 of file x509.py.

#### 13.237.2.6 def rpki.x509.X509.getIssuer ( self )

Get the issuer of this certificate.

Definition at line 453 of file x509.py.

#### 13.237.2.7 def rpki.x509.X509.getNotAfter ( self )

Get the expiration time of this certificate.

Definition at line 471 of file x509.py.

#### 13.237.2.8 def rpki.x509.X509.getNotBefore ( self )

Get the inception time of this certificate.

Definition at line 465 of file x509.py.

**13.237.2.9 def rpki.x509.X509.getPublicKey ( self )**

Extract the public key from this certificate.

Definition at line 483 of file x509.py.

**13.237.2.10 def rpki.x509.X509.getSerial ( self )**

Get the serial number of this certificate.

Definition at line 477 of file x509.py.

**13.237.2.11 def rpki.x509.X509.getSubject ( self )**

Get the subject of this certificate.

Definition at line 459 of file x509.py.

**13.237.2.12 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 495 of file x509.py.

**13.237.2.13 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 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 585 of file x509.py.

### 13.237.3 Member Data Documentation

#### 13.237.3.1 rpki.x509.X509.DER

DER value of this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 420 of file x509.py.

```
13.237.3.2 tuple rpki.x509.X509.formats = ("DER", "POW", "POWpkix")
[static]
```

Formats supported in this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 415 of file x509.py.

```
13.237.3.3 tuple rpki.x509.X509.pem_converter =
PEM_converter("CERTIFICATE") [static]
```

PEM converter for this object.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 416 of file x509.py.

#### 13.237.3.4 rpki.x509.X509.POW

Definition at line 435 of file x509.py.

#### 13.237.3.5 rpki.x509.X509.POWpkix

Definition at line 444 of file x509.py.

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

- [x509.py \(3793\)](#)

## 13.238 rpki.x509.XML\_CMS\_object Class Reference

Inheritance diagram for rpki.x509.XML\_CMS\_object:

Collaboration diagram for rpki.x509.XML\_CMS\_object:

### Public Member Functions

- def [decode](#)
- def [dump\\_to\\_disk](#)
- def [encode](#)
- def [pretty\\_print\\_content](#)
- def [schema\\_check](#)
- def [unwrap](#)
- def [wrap](#)

### Public Attributes

- [content](#)

### Static Public Attributes

- [dump\\_inbound\\_cms](#) = None  
*If set, we write all inbound XML-CMS PDUs to disk, for debugging.*
- [dump\\_outbound\\_cms](#) = None  
*If set, we write all outbound XML-CMS PDUs to disk, for debugging.*
- tuple [econtent\\_oid](#) = POWify\_OID("id-ct-xml")

### 13.238.1 Detailed Description

Class to hold CMS-wrapped XML protocol data.

Definition at line 1144 of file x509.py.

### 13.238.2 Member Function Documentation

#### 13.238.2.1 def rpki.x509.XML\_CMS\_object.decode ( self, xml )

Decode XML and set inner content.

Definition at line 1169 of file x509.py.

#### 13.238.2.2 def rpki.x509.XML\_CMS\_object.dump\_to\_disk ( *self*, *prefix* )

Write DER of current message to disk, for debugging.

Definition at line 1193 of file x509.py.

#### 13.238.2.3 def rpki.x509.XML\_CMS\_object.encode ( *self* )

Encode inner content for signing.

Definition at line 1163 of file x509.py.

#### 13.238.2.4 def rpki.x509.XML\_CMS\_object.pretty\_print\_content ( *self* )

Pretty print XML content of this message.

Definition at line 1175 of file x509.py.

#### 13.238.2.5 def rpki.x509.XML\_CMS\_object.schema\_check ( *self* )

Handle XML RelaxNG schema check.

Definition at line 1181 of file x509.py.

#### 13.238.2.6 def rpki.x509.XML\_CMS\_object.unwrap ( *self*, *ta* )

Unwrap a CMS-wrapped XML PDU and return Python objects.

Definition at line 1213 of file x509.py.

**13.238.2.7** `def rpki.x509.XML_CMS_object.wrap ( self, msg, keypair, certs, crls = None )`

Wrap an XML PDU in CMS and return its DER encoding.

Definition at line 1201 of file x509.py.

### 13.238.3 Member Data Documentation

#### 13.238.3.1 rpki.x509.XML\_CMS\_object.content

Reimplemented from [rpki.x509.CMS\\_object](#).

Definition at line 1171 of file x509.py.

**13.238.3.2** `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 1161 of file x509.py.

**13.238.3.3** `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 1155 of file x509.py.

**13.238.3.4** `tuple rpki.x509.XML_CMS_object.econtent_oid =`  
`POWify_OID("id-ct-xml") [static]`

Reimplemented from [rpki.x509.CMS\\_object](#).

Definition at line 1149 of file x509.py.

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

- [x509.py \(3793\)](#)

## 13.239 rpki.xml\_utils.base\_elt Class Reference

Inheritance diagram for rpki.xml\_utils.base\_elt:

Collaboration diagram for rpki.xml\_utils.base\_elt:

### Public Member Functions

- def [\\_\\_str\\_\\_](#)
- def [endElement](#)
- def [make\\_b64elt](#)
- def [make\\_elt](#)
- def [make\\_pdu](#)
- def [read\\_attrs](#)
- def [startElement](#)
- def [toXML](#)

### Static Public Attributes

- tuple [attributes](#) = ()  
*XML attributes for this element.*
- tuple [booleans](#) = ()  
*Boolean attributes (value "yes" or "no") for this element.*
- tuple [elements](#) = ()  
*XML elements contained by this element.*

### 13.239.1 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 132 of file xml\_utils.py.

### 13.239.2 Member Function Documentation

#### 13.239.2.1 def rpki.xml\_utils.base\_elt.\_\_str\_\_ ( *self* )

Convert a base\_elt object to string format.

Reimplemented in [rpki.publication.report\\_error\\_elt](#).

Definition at line 205 of file xml\_utils.py.

#### 13.239.2.2 def rpki.xml\_utils.base\_elt.endElement ( *self*, *stack*, *name*, *text* )

Default endElement() handler: just pop the stack.

Reimplemented in [rpki.publication.publication\\_object\\_elt](#), [rpki.xml\\_utils.text\\_elt](#), and [rpki.xml\\_utils.data\\_elt](#).

Definition at line 159 of file xml\_utils.py.

#### 13.239.2.3 def rpki.xml\_utils.base\_elt.make\_b64elt ( *self*, *elt*, *name*, *value* )

Constructor for Base64-encoded subelement.

Definition at line 198 of file xml\_utils.py.

#### 13.239.2.4 def rpki.xml\_utils.base\_elt.make\_elt ( *self* )

XML element constructor.

Definition at line 184 of file xml\_utils.py.

#### 13.239.2.5 def rpki.xml\_utils.base\_elt.make\_pdu ( *cls*, *kargs* )

Generic PDU constructor.

Definition at line 212 of file xml\_utils.py.



### 13.239.2.6 def rpki.xml\_utils.base\_elt.read\_attrs ( self, attrs )

Template-driven attribute reader.

Definition at line 172 of file xml\_utils.py.

### 13.239.2.7 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 151 of file xml\_utils.py.

### 13.239.2.8 def rpki.xml\_utils.base\_elt.toXML ( self )

Default toXML() element generator.

Reimplemented in [rpki.left\\_right.list\\_resources\\_elt](#), [rpki.publication.publication\\_object\\_elt](#), [rpki.xml\\_utils.text\\_elt](#), and [rpki.xml\\_utils.data\\_elt](#).

Definition at line 166 of file xml\_utils.py.

## 13.239.3 Member Data Documentation

### 13.239.3.1 rpki::xml\_utils.base\_elt::attributes = () [static]

XML attributes for this element.

Reimplemented in [rpki.left\\_right.self\\_elt](#), [rpki.left\\_right.bsc\\_elt](#), [rpki.left\\_right.repository\\_elt](#), [rpki.left\\_right.parent\\_elt](#), [rpki.left\\_right.child\\_elt](#), [rpki.left\\_right.list\\_resources\\_elt](#), [rpki.left\\_right.list\\_roa\\_requests\\_elt](#), [rpki.left\\_right.list\\_ghostbuster\\_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 141 of file xml\_utils.py.

### 13.239.3.2 rpki::xml\_utils.base\_elt::booleans = () [static]

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

Reimplemented in [rpki.left\\_right.self\\_elt](#), [rpki.left\\_right.bsc\\_elt](#), [rpki.left\\_right.parent\\_elt](#), and [rpki.left\\_right.child\\_elt](#).

Definition at line 149 of file [xml\\_utils.py](#).

### 13.239.3.3 rpki::xml\_utils.base\_elt::elements = () [static]

XML elements contained by this element.

Reimplemented in [rpki.left\\_right.self\\_elt](#), [rpki.left\\_right.bsc\\_elt](#), [rpki.left\\_right.repository\\_elt](#), [rpki.left\\_right.parent\\_elt](#), [rpki.left\\_right.child\\_elt](#), [rpki.publication.config\\_elt](#), and [rpki.publication.client\\_elt](#).

Definition at line 145 of file [xml\\_utils.py](#).

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

- [xml\\_utils.py \(3725\)](#)

## 13.240 rpki.xml\_utils.data\_elt Class Reference

Inheritance diagram for [rpki.xml\\_utils.data\\_elt](#):

Collaboration diagram for [rpki.xml\\_utils.data\\_elt](#):

### Public Member Functions

- def [endElement](#)
- def [make\\_reply](#)
- def [make\\_reply\\_clone\\_hook](#)
- def [serve\\_create](#)
- def [serve\\_destroy](#)
- def [serve\\_destroy\\_hook](#)
- def [serve\\_dispatch](#)
- def [serve\\_fetch\\_one](#)
- def [serve\\_get](#)
- def [serve\\_list](#)
- def [serve\\_post\\_save\\_hook](#)
- def [serve\\_pre\\_save\\_hook](#)

- def [serve\\_set](#)
- def [toXML](#)
- def [unimplemented\\_control](#)

### 13.240.1 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 247 of file xml\_utils.py.

### 13.240.2 Member Function Documentation

#### 13.240.2.1 def rpki.xml\_utils.data\_elt.endElement ( *self*, *stack*, *name*, *text* )

Default endElement handler for SQL-based objects. This assumes that sub-elements are Base64-encoded using the sql\_template mechanism.

Reimplemented from [rpki.xml\\_utils.base\\_elt](#).

Definition at line 253 of file xml\_utils.py.

#### 13.240.2.2 def rpki.xml\_utils.data\_elt.make\_reply ( *self*, *r\_pdu* = *None* )

Construct a reply PDU.

Definition at line 277 of file xml\_utils.py.

#### 13.240.2.3 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 294 of file xml\_utils.py.

**13.240.2.4 def rpki.xml\_utils.data\_elt.serve\_create ( self, r\_msg, cb, eb )**

Handle a create action.

Definition at line 322 of file xml\_utils.py.

**13.240.2.5 def rpki.xml\_utils.data\_elt.serve\_destroy ( self, r\_msg, cb, eb )**

Handle a destroy action.

Definition at line 392 of file xml\_utils.py.

**13.240.2.6 def rpki.xml\_utils.data\_elt.serve\_destroy\_hook ( self, cb, eb )**

Overridable hook.

Reimplemented in [rpki.left\\_right.child\\_elt](#).

Definition at line 386 of file xml\_utils.py.

**13.240.2.7 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 403 of file xml\_utils.py.

**13.240.2.8 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 300 of file xml\_utils.py.

**13.240.2.9** `def rpki.xml_utils.data_elt.serve_get ( self, r_msg, cb, eb )`

Handle a get action.

Definition at line 368 of file xml\_utils.py.

**13.240.2.10** `def rpki.xml_utils.data_elt.serve_list ( self, r_msg, cb, eb )`

Handle a list action for non-self objects.

Definition at line 377 of file xml\_utils.py.

**13.240.2.11** `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](#), and [rpki.left\\_right.child\\_elt](#).

Definition at line 316 of file xml\_utils.py.

**13.240.2.12** `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 310 of file xml\_utils.py.

**13.240.2.13** `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 345 of file xml\_utils.py.

**13.240.2.14 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 267 of file xml\_utils.py.

**13.240.2.15 def rpki.xml\_utils.data\_elt.unimplemented\_control ( self, controls )**

Uniform handling for unimplemented control operations.

Definition at line 416 of file xml\_utils.py.

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

- [xml\\_utils.py \(3725\)](#)

**13.241 rpki.xml\_utils.msg Class Reference**

Inheritance diagram for rpki.xml\_utils.msg:

Collaboration diagram for rpki.xml\_utils.msg:

**Public Member Functions**

- def [\\_\\_str\\_\\_](#)
- def [endElement](#)
- def [is\\_query](#)
- def [is\\_reply](#)
- def [query](#)
- def [reply](#)
- def [startElement](#)
- def [toXML](#)

**Public Attributes**

- [type](#)
- [version](#)

### 13.241.1 Detailed Description

Generic top-level PDU.

Definition at line 424 of file xml\_utils.py.

### 13.241.2 Member Function Documentation

#### 13.241.2.1 def rpki.xml\_utils.msg.\_\_str\_\_( self )

Convert msg object to string.

Definition at line 450 of file xml\_utils.py.

#### 13.241.2.2 def rpki.xml\_utils.msg.endElement( self, stack, name, text )

Handle top-level PDU.

Definition at line 442 of file xml\_utils.py.

#### 13.241.2.3 def rpki.xml\_utils.msg.is\_query( self )

Is this msg a query?

Definition at line 482 of file xml\_utils.py.

#### 13.241.2.4 def rpki.xml\_utils.msg.is\_reply( self )

Is this msg a reply?

Definition at line 488 of file xml\_utils.py.

**13.241.2.5 def rpki.xml\_utils.msg.query ( *cls*, *args* )**

Create a query PDU.

Definition at line 465 of file xml\_utils.py.

**13.241.2.6 def rpki.xml\_utils.msg.reply ( *cls*, *args* )**

Create a reply PDU.

Definition at line 474 of file xml\_utils.py.

**13.241.2.7 def rpki.xml\_utils.msg.startElement ( *self*, *stack*, *name*, *attrs* )**

Handle top-level PDU.

Definition at line 429 of file xml\_utils.py.

**13.241.2.8 def rpki.xml\_utils.msg.toXML ( *self* )**

Generate top-level PDU.

Definition at line 456 of file xml\_utils.py.

**13.241.3 Member Data Documentation****13.241.3.1 rpki.xml\_utils.msg.type**

Definition at line 431 of file xml\_utils.py.

**13.241.3.2 rpki.xml\_utils.msg.version**



Reimplemented in [rpki.left\\_right.msg](#), and [rpki.publication.msg](#).

Definition at line 431 of file `xml_utils.py`.

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

- [xml\\_utils.py \(3725\)](#)

## 13.242 rpki.xml\_utils.sax\_handler Class Reference

Inheritance diagram for `rpki.xml_utils.sax_handler`:

Collaboration diagram for `rpki.xml_utils.sax_handler`:

### Public Member Functions

- [def \\_\\_init\\_\\_](#)
- [def characters](#)
- [def create\\_top\\_level](#)
- [def endElement](#)
- [def endElementNS](#)
- [def saxify](#)
- [def startElement](#)
- [def startElementNS](#)

### Public Attributes

- [result](#)
- [stack](#)
- [text](#)

### 13.242.1 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`.

### 13.242.2 Constructor & Destructor Documentation

#### 13.242.2.1 `def rpki.xml_utils.sax_handler.__init__ ( self )`

Initialize SAX handler.

Definition at line 53 of file xml\_utils.py.

### 13.242.3 Member Function Documentation

#### 13.242.3.1 `def rpki.xml_utils.sax_handler.characters ( self, content )`

Accumulate a chunk of element content (text).

Definition at line 73 of file xml\_utils.py.

#### 13.242.3.2 `def rpki.xml_utils.sax_handler.create_top_level ( self, name, attrs )`

Handle top-level PDU for this protocol.

Definition at line 125 of file xml\_utils.py.

#### 13.242.3.3 `def rpki.xml_utils.sax_handler.endElement ( self, name )`

Handle endElement() events. Mostly this means handling any accumulated element text.

Definition at line 107 of file xml\_utils.py.

#### 13.242.3.4 `def rpki.xml_utils.sax_handler.endElementNS ( self, name, qname )`

Redirect endElementNS() events to endElement().

Definition at line 67 of file xml\_utils.py.

### 13.242.3.5 def rpki.xml\_utils.sax\_handler.saxify ( *cls*, *elt* )

Create a one-off SAX parser, parse an ETree, return the result.

Definition at line 117 of file xml\_utils.py.

### 13.242.3.6 def rpki.xml\_utils.sax\_handler.startElement ( *self*, *name*, *attrs* )

Handle startElement() events.

We maintain a stack of nested elements under construction so that we can feed events directly to the current element rather than having to pass them through all the nesting elements.

If the stack is empty, this event is for the outermost element, so we call a virtual method to create the corresponding object and that's the object we'll be returning as our final result.

Definition at line 79 of file xml\_utils.py.

### 13.242.3.7 def rpki.xml\_utils.sax\_handler.startElementNS ( *self*, *name*, *qname*, *attrs* )

Redirect startElementNS() events to startElement().

Definition at line 61 of file xml\_utils.py.

## 13.242.4 Member Data Documentation

### 13.242.4.1 rpki.xml\_utils.sax\_handler.result

Definition at line 89 of file xml\_utils.py.

### 13.242.4.2 rpki.xml\_utils.sax\_handler.stack

Definition at line 55 of file xml\_utils.py.

### 13.242.4.3 rpki.xml\_utils.sax\_handler.text

Definition at line 55 of file xml\_utils.py.

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

- [xml\\_utils.py \(3725\)](#)

### 13.243 rpki.xml\_utils.text\_elt Class Reference

Inheritance diagram for rpki.xml\_utils.text\_elt:

Collaboration diagram for rpki.xml\_utils.text\_elt:

#### Public Member Functions

- def [endElement](#)
- def [toXML](#)

#### Static Public Attributes

- [text\\_attribute](#) = None  
*Name of the class attribute that holds the text value.*

#### 13.243.1 Detailed Description

Virtual base class for XML message elements that contain text.

Definition at line 223 of file xml\_utils.py.

#### 13.243.2 Member Function Documentation

##### 13.243.2.1 def rpki.xml\_utils.text\_elt.endElement ( self, stack, name, text )

Extract text from parsed XML.

Reimplemented from [rpki.xml\\_utils.base\\_elt](#).

Definition at line 232 of file xml\_utils.py.

### 13.243.2.2 `def rpki.xml_utils.text_elt.toXML ( self )`

Insert text into generated XML.

Reimplemented from [rpki.xml\\_utils.base\\_elt](#).

Definition at line 239 of file `xml_utils.py`.

### 13.243.3 Member Data Documentation

#### 13.243.3.1 `rpki::xml_utils.text_elt::text_attribute = None [static]`

Name of the class attribute that holds the text value.

Reimplemented in [rpki.left\\_right.list\\_ghostbuster\\_requests\\_elt](#), [rpki.left\\_right.list\\_published\\_objects\\_elt](#), [rpki.left\\_right.report\\_error\\_elt](#), and [rpki.publication.report\\_error\\_elt](#).

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

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

- [xml\\_utils.py \(3725\)](#)

### 13.244 Sequence Class Reference

Inheritance diagram for Sequence:

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

- [roa.py \(3598\)](#)

### 13.245 SequenceOf Class Reference

Inheritance diagram for SequenceOf:

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

- [roa.py \(3598\)](#)

### 13.246 set Class Reference

Inheritance diagram for set:

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

- [myrpki.py \(3793\)](#)

### 13.247 TextWrapper Class Reference

Inheritance diagram for TextWrapper:

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

- [irbe\\_cli.py \(3711\)](#)

### 13.248 ContentHandler Class Reference

Inheritance diagram for ContentHandler:

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

- [xml\\_utils.py \(3725\)](#)

## 14 File Documentation

### 14.1 \_\_doc\_\_.py File Reference

#### Packages

- package [rpki.\\_\\_doc\\_\\_](#)

#### 14.1.1 Detailed Description

Documentation sourc, expressed as Python comments to make Doxygen happy.

#### Id:

[\\_\\_doc\\_\\_.py](#) 3853 2011-06-06 14:31:57Z 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](#).

## 14.2 `__init__.py` File Reference

### Packages

- package [rpki](#)

## 14.3 `adns.py` File Reference

### Classes

- class [rpki.adns.dispatcher](#)
- class [rpki.adns.getaddrinfo](#)
- class [rpki.adns.query](#)
- class [rpki.adns.test\\_getaddrinfo](#)
- class [rpki.adns.test\\_query](#)

### Packages

- package [rpki.adns](#)

### Variables

- list [rpki::adns.nameservers](#) = []

*Nameservers from `resolver.nameservers` converted to (af, address) pairs.*

- tuple `rpki::adns.resolver` = `dns.resolver.Resolver()`  
*Resolver object, shared by everything using this module.*

## 14.4 `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`

## 14.5 `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

**14.6 config.py File Reference****Classes**

- class [rpki.config.parser](#)

**Packages**

- package [rpki.config](#)

**Variables**

- [rpki::config.default\\_dirname](#) = None  
*Default name of directory to check for global config file, or None if no global config file.*
- string [rpki::config.default\\_envname](#) = "RPKI\_CONF"  
*Name of environment variable containing config file name.*
- string [rpki::config.default\\_filename](#) = "rpki.conf"  
*Default name of config file if caller doesn't specify one explicitly.*

**14.7 exceptions.py File Reference****Classes**

- class [rpki.exceptions.BadClassNameSyntax](#)

- class [rpki.exceptions.BadClientURL](#)
- class [rpki.exceptions.BadContactURL](#)
- class [rpki.exceptions.BadExtension](#)
- class [rpki.exceptions.BadIPResource](#)
- class [rpki.exceptions.BadIRDBReply](#)
- class [rpki.exceptions.BadIssueResponse](#)
- class [rpki.exceptions.BadPKCS10](#)
- class [rpki.exceptions.BadPublicationReply](#)
- class [rpki.exceptions.BadQuery](#)
- class [rpki.exceptions.BadROAPrefix](#)
- class [rpki.exceptions.BadSender](#)
- class [rpki.exceptions.BadStatusCode](#)
- class [rpki.exceptions.BadURISyntax](#)
- class [rpki.exceptions.BSCNotFound](#)
- class [rpki.exceptions.BSCNotReady](#)
- class [rpki.exceptions.ChildNotFound](#)
- class [rpki.exceptions.ClassNameMismatch](#)
- class [rpki.exceptions.ClassNameUnknown](#)
- class [rpki.exceptions.ClientNotFound](#)
- class [rpki.exceptions.CMSContentNotSet](#)
- class [rpki.exceptions.CMSCRLNotSet](#)
- class [rpki.exceptions.CMSVerificationFailed](#)
- class [rpki.exceptions.CommandParseFailure](#)
- class [rpki.exceptions.DBConsistencyError](#)
- class [rpki.exceptions.DEROBJECTConversionError](#)
- class [rpki.exceptions.DuplicateObject](#)
- class [rpki.exceptions.EmptyPEM](#)
- class [rpki.exceptions.EmptyROAPrefixList](#)
- class [rpki.exceptions.ForbiddenURI](#)
- class [rpki.exceptions.HandleTranslationError](#)
- class [rpki.exceptions.HTTPBadVersion](#)
- class [rpki.exceptions.HTTPClientAborted](#)
- class [rpki.exceptions.HTTPRequestFailed](#)
- class [rpki.exceptions.HTTPTimeout](#)
- class [rpki.exceptions.HTTPUnexpectedState](#)
- class [rpki.exceptions.MissingCMSCRL](#)
- class [rpki.exceptions.MissingCMSEECert](#)
- class [rpki.exceptions.MultipleTLSEECert](#)
- class [rpki.exceptions.MustBePrefix](#)
- class [rpki.exceptions.NoActiveCA](#)
- class [rpki.exceptions.NoCoveringCertForROA](#)
- class [rpki.exceptions.NoObjectAtURI](#)
- class [rpki.exceptions.NotACertificateChain](#)

- class [rpki.exceptions.NotFound](#)
- class [rpki.exceptions.NotImplementedYet](#)
- class [rpki.exceptions.NotInDatabase](#)
- class [rpki.exceptions.ReceivedTLSCACert](#)
- class [rpki.exceptions.RPKI\\_Exception](#)
- class [rpki.exceptions.ServerShuttingDown](#)
- class [rpki.exceptions.SKIMismatch](#)
- class [rpki.exceptions.SubprocessError](#)
- class [rpki.exceptions.TLSValidationError](#)
- class [rpki.exceptions.UnexpectedCMSCerts](#)
- class [rpki.exceptions.UnexpectedCMSCRLs](#)
- class [rpki.exceptions.UnparsableCMSDER](#)
- class [rpki.exceptions.UpstreamError](#)
- class [rpki.exceptions.WrongEContentType](#)

#### Packages

- package [rpki.exceptions](#)

## 14.8 http.py File Reference

#### Classes

- class [rpki.http.caller](#)
- class [rpki.http.http\\_client](#)
- class [rpki.http.http\\_listener](#)
- class [rpki.http.http\\_message](#)
- class [rpki.http.http\\_queue](#)
- class [rpki.http.http\\_request](#)
- class [rpki.http.http\\_response](#)
- class [rpki.http.http\\_server](#)
- class [rpki.http.http\\_stream](#)

#### Packages

- package [rpki.http](#)

### Functions

- def `rpki::http.addr_to_string`
- def `rpki::http.client`
- def `rpki::http.localhost_addrinfo`
- def `rpki::http.log_method`
- def `rpki::http.server`
- def `rpki::http.supported_address_families`

### Variables

- dictionary `rpki::http.client_queues` = { }  
*Map of (host, port) tuples to `http_queue` objects.*
- `rpki::http.debug_http` = False  
*Verbose chatter about HTTP streams.*
- tuple `rpki::http.default_client_timeout` = `rpki.sundial.timedelta(minutes = 15)`  
*Default HTTP client connection timeout.*
- tuple `rpki::http.default_http_version` = (1, 0)  
*Preferred HTTP version.*
- tuple `rpki::http.default_server_timeout` = `rpki.sundial.timedelta(minutes = 20)`  
*Default HTTP server connection timeouts.*
- int `rpki::http.default_tcp_port` = 80  
*Default port for clients and servers that don't specify one.*
- `rpki::http.enable_ipv6_clients` = False  
*Whether to consider IPv6 addresses when making connections.*
- `rpki::http.enable_ipv6_servers` = True  
*Whether to enable IPv6 listeners.*
- `rpki::http.have_ipv6` = False  
*Whether the current machine claims to support IPv6.*
- string `rpki::http.rpki_content_type` = "application/x-rpki"  
*HTTP content type used for all RPKI messages.*
- `rpki::http.use_adns` = False

Whether to use [rpki.adns](#) code.

- [rpki::http.want\\_persistent\\_client](#) = False

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

- [rpki::http.want\\_persistent\\_server](#) = False

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

## 14.9 ipaddrs.py File Reference

### Classes

- class [rpki.ipaddrs.v4addr](#)
- class [rpki.ipaddrs.v6addr](#)

### Packages

- package [rpki.ipaddrs](#)

### Functions

- def [rpki::ipaddrs.parse](#)

## 14.10 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.cfg](#) = [rpki.config.parser](#)(cfg\_file, "irbe\_cli")
- [irbe\\_cli.cfg\\_file](#) = None
- tuple [irbe\\_cli.client\\_cert](#) = [rpki.x509.X509](#)(Auto\_file = cfg.get("rpkid-irbe-cert"))
- tuple [irbe\\_cli.client\\_key](#) = [rpki.x509.RSA](#)( Auto\_file = cfg.get("rpkid-irbe-key"))
- [irbe\\_cli.debug](#) = verbose))
- [irbe\\_cli.pem\\_out](#) = None
- [irbe\\_cli.proto](#) = left\_right\_proto,
- [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]]
- tuple [irbe\\_cli.server\\_cert](#) = [rpki.x509.X509](#)(Auto\_file = cfg.get("rpkid-cert"))
- tuple [irbe\\_cli.server\\_ta](#) = [rpki.x509.X509](#)(Auto\_file = cfg.get("rpkid-bpki-ta"))
- list [irbe\\_cli.top\\_opts](#) = ["config=", "help", "pem\_out=", "quiet", "verbose"]
- tuple [irbe\\_cli.url](#) = cfg.get("rpkid-url")
- tuple [irbe\\_cli.usage\\_fill](#) = UsageWrapper(subsequent\_indent = " " \* 4)
- [irbe\\_cli.verbose](#) = True

## 14.11 irdbd.py File Reference

### Classes

- class [rpki.irdbd.main](#)

### Packages

- package [rpki.irdbd](#)

## 14.12 irdbd.py File Reference

### Packages

- package [irdbd](#)

## 14.13 left\_right.py File Reference

### Classes

- class [rpki.left\\_right.bsc\\_elt](#)
- class [rpki.left\\_right.child\\_elt](#)
- class [rpki.left\\_right.cms\\_msg](#)
- class [rpki.left\\_right.data\\_elt](#)
- class [rpki.left\\_right.left\\_right\\_namespace](#)
- class [rpki.left\\_right.list\\_ghostbuster\\_requests\\_elt](#)
- 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

**14.14 log.py File Reference****Classes**

- class `rpki.log.logger`

**Packages**

- package `rpki.log`

**Functions**

- def `rpki::log.init`
- def `rpki::log.log_repr`
- def `rpki::log.set_trace`
- def `rpki::log.trace`
- def `rpki::log.traceback`

**Variables**

- tuple `rpki::log.debug` = `logger(syslog.LOG_DEBUG)`
- `rpki::log.enable_trace` = False  
*Whether call tracing is enabled.*
- tuple `rpki::log.error` = `logger(syslog.LOG_ERR)`
- tuple `rpki::log.info` = `logger(syslog.LOG_INFO)`
- tuple `rpki::log.note` = `logger(syslog.LOG_NOTICE)`
- int `rpki::log.pid` = 0
- `rpki::log.show_python_ids` = False  
*Whether `__repr__()` methods should show Python id numbers.*
- string `rpki::log.tag` = ""
- `rpki::log.use_syslog` = True  
*Whether to use syslog.*
- tuple `rpki::log.warn` = `logger(syslog.LOG_WARNING)`



## 14.15 manifest.py File Reference

### Classes

- class [rpki.manifest.FileAndHash](#)
- class [rpki.manifest.FilesAndHashes](#)
- class [rpki.manifest.Manifest](#)

### Packages

- package [rpki.manifest](#)

## 14.16 myrpki.py File Reference

### Classes

- class [rpki.myrpki.CA](#)
- class [rpki.myrpki.child](#)
- class [rpki.myrpki.children](#)
- class [rpki.myrpki.comma\\_set](#)
- class [rpki.myrpki.csv\\_reader](#)
- class [rpki.myrpki.csv\\_writer](#)
- class [rpki.myrpki.EntityDB](#)
- class [rpki.myrpki.IRDB](#)
- class [rpki.myrpki.main](#)
- class [rpki.myrpki.parent](#)
- class [rpki.myrpki.parents](#)
- class [rpki.myrpki.repositories](#)
- class [rpki.myrpki.repository](#)
- class [rpki.myrpki.roa\\_request](#)
- class [rpki.myrpki.roa\\_requests](#)

### Packages

- package [rpki.myrpki](#)

### Functions

- def [rpki::myrpki.b64\\_equal](#)
- def [rpki::myrpki.etree\\_post\\_read](#)
- def [rpki::myrpki.etree\\_pre\\_write](#)
- def [rpki::myrpki.etree\\_read](#)

- def `rpki::myrpki.etree_validate`
- def `rpki::myrpki.etree_write`
- def `rpki::myrpki.PEMBase64`
- def `rpki::myrpki.PEMElement`

#### Variables

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

### 14.17 `oids.py` File Reference

#### Packages

- package `rpki.oids`

#### Variables

- tuple `rpki::oids.name2oid` = `dict((v, k) for k, v in oid2name.items())`  
*Mapping table of string names to OIDs.*
- dictionary `rpki::oids.oid2name`  
*Mapping table of OIDs to conventional string names.*

### 14.18 `pubd.py` File Reference

#### Classes

- class `rpki.pubd.main`

#### Packages

- package `rpki.pubd`

## 14.19 pubd.py File Reference

### Packages

- package [pubd](#)

## 14.20 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.ghostbuster\\_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](#)

## 14.21 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.*

## 14.22 resource\_set.py File Reference

### Classes

- class [rpki.resource\\_set.resource\\_bag](#)
- class [rpki.resource\\_set.resource\\_range](#)
- class [rpki.resource\\_set.resource\\_range\\_as](#)
- class [rpki.resource\\_set.resource\\_range\\_ip](#)
- class [rpki.resource\\_set.resource\\_range\\_ipv4](#)
- class [rpki.resource\\_set.resource\\_range\\_ipv6](#)
- class [rpki.resource\\_set.resource\\_set](#)
- class [rpki.resource\\_set.resource\\_set\\_as](#)
- class [rpki.resource\\_set.resource\\_set\\_ip](#)
- class [rpki.resource\\_set.resource\\_set\\_ipv4](#)
- class [rpki.resource\\_set.resource\\_set\\_ipv6](#)
- class [rpki.resource\\_set.roa\\_prefix](#)
- class [rpki.resource\\_set.roa\\_prefix\\_ipv4](#)
- class [rpki.resource\\_set.roa\\_prefix\\_ipv6](#)
- class [rpki.resource\\_set.roa\\_prefix\\_set](#)
- class [rpki.resource\\_set.roa\\_prefix\\_set\\_ipv4](#)
- class [rpki.resource\\_set.roa\\_prefix\\_set\\_ipv6](#)

### Packages

- package [rpki.resource\\_set](#)

### Functions

- def [rpki::resource\\_set.\\_bs2long](#)
- def [rpki::resource\\_set.\\_long2bs](#)
- def [rpki::resource\\_set.\\_rsplit](#)
- def [rpki::resource\\_set.test1](#)
- def [rpki::resource\\_set.test2](#)
- def [rpki::resource\\_set.test3](#)
- def [rpki::resource\\_set.testprefix](#)

**Variables**

- string `rpki::resource_set.inherit_token` = "<inherit>"  
*Token used to indicate inheritance in read and print syntax.*
- tuple `rpki::resource_set.re_address_range` = `re.compile("^[0-9:.a-fA-F]+)-([0-9:.a-fA-F]+)$")`
- tuple `rpki::resource_set.re_asn_range` = `re.compile("^[0-9]+)-([0-9]+)$")`
- tuple `rpki::resource_set.re_prefix` = `re.compile("^[0-9:.a-fA-F]+)/([0-9]+)$")`
- tuple `rpki::resource_set.re_prefix_with_maxlen` = `re.compile("^[0-9:.a-fA-F]+)/([0-9]+)-([0-9]+)$")`

**14.23 roa.py File Reference****Classes**

- class `rpki.roa.ROAIPAddress`
- class `rpki.roa.ROAIPAddresses`
- class `rpki.roa.ROAIPAddressFamilies`
- class `rpki.roa.ROAIPAddressFamily`
- class `rpki.roa.RouteOriginAttestation`

**Packages**

- package `rpki.roa`

**14.24 rootd.py File Reference****Classes**

- class `rpki.rootd.cms_msg`
- class `rpki.rootd.issue_pdu`
- class `rpki.rootd.list_pdu`
- class `rpki.rootd.main`
- class `rpki.rootd.message_pdu`
- class `rpki.rootd.revoke_pdu`
- class `rpki.rootd.sax_handler`

**Packages**

- package `rpki.rootd`

**Variables**

- `rpki::rootd.rootd` = None

**14.25 rootd.py File Reference****Packages**

- package `rootd`

**14.26 rpki.py File Reference****Classes**

- class `rpki.rpki.ca_detail_obj`
- class `rpki.rpki.ca_obj`
- class `rpki.rpki.child_cert_obj`
- class `rpki.rpki.ghostbuster_obj`
- class `rpki.rpki.main`
- class `rpki.rpki.publication_queue`
- class `rpki.rpki.revoked_cert_obj`
- class `rpki.rpki.roa_obj`

**Packages**

- package `rpki.rpki`

**14.27 rpki.py File Reference****Packages**

- package `rpki`

**14.28 sql.py File Reference****Classes**

- class `rpki.sql.session`
- class `rpki.sql.sql_persistent`
- class `rpki.sql.template`

**Packages**

- package [rpki.sql](#)

**14.29 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](#)

**14.30 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.nsmmap](#) = { None : xmlns }
- string [rpki::up\\_down.xmlns](#) = "http://www.apnic.net/specs/rescerts/up-down/"

**14.31 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.Ghostbuster](#)
- 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.base64\\_with\\_linebreaks](#)
- def [rpki::x509.calculate\\_SKI](#)
- def [rpki::x509.POWify\\_OID](#)



## 14.32 xml\_utils.py File Reference

### Classes

- class [rpki.xml\\_utils.base\\_elt](#)
- class [rpki.xml\\_utils.data\\_elt](#)
- class [rpki.xml\\_utils.msg](#)
- class [rpki.xml\\_utils.sax\\_handler](#)
- class [rpki.xml\\_utils.text\\_elt](#)

### Packages

- package [rpki.xml\\_utils](#)

## Index

- `__abs__`
  - `rpki::sundial::timedelta`, 431
- `__add__`
  - `rpki::sundial::datetime`, 426
  - `rpki::sundial::timedelta`, 431
- `__call__`
  - `irbe_cli::UsageWrapper`, 129
  - `rpki::async::iterator`, 145
  - `rpki::async::sync_wrapper`, 147
  - `rpki::http::caller`, 184
  - `rpki::log::logger`, 260
  - `rpki::myrpki::EntityDB`, 279
- `__cmp__`
  - `rpki::async::timer`, 150
  - `rpki::resource_set::resource_range`, 330
  - `rpki::resource_set::roa_prefix`, 348
  - `rpki::x509::DER_object`, 474
- `__del__`
  - `rpki::async::timer`, 150
- `__div__`
  - `rpki::sundial::timedelta`, 431
- `__doc__` `py(3853)`, 519
- `__eq__`
  - `rpki::resource_set::resource_bag`, 327
- `__floordiv__`
  - `rpki::sundial::timedelta`, 431
- `__getattr__`
  - `rpki::myrpki::csv_writer`, 277
- `__init__`
  - `rpki::adns::dispatcher`, 131
  - `rpki::adns::getaddrinfo`, 133
  - `rpki::adns::query`, 136
  - `rpki::adns::test_getaddrinfo`, 140
  - `rpki::adns::test_query`, 142
  - `rpki::async::gc_summary`, 143
  - `rpki::async::iterator`, 145
  - `rpki::async::sync_wrapper`, 147
  - `rpki::async::timer`, 150
  - `rpki::cli::Cmd`, 155
  - `rpki::config::parser`, 159
  - `rpki::http::caller`, 184
  - `rpki::http::http_client`, 186
  - `rpki::http::http_listener`, 191
  - `rpki::http::http_message`, 193
  - `rpki::http::http_queue`, 196
  - `rpki::http::http_request`, 199
  - `rpki::http::http_response`, 201
  - `rpki::http::http_server`, 203
  - `rpki::http::http_stream`, 206
  - `rpki::irdbd::main`, 215
  - `rpki::log::logger`, 260
  - `rpki::manifest::FileAndHash`, 261
  - `rpki::manifest::FilesAndHashes`, 262
  - `rpki::manifest::Manifest`, 263
  - `rpki::myrpki::CA`, 265
  - `rpki::myrpki::child`, 271
  - `rpki::myrpki::csv_reader`, 275
  - `rpki::myrpki::csv_writer`, 277
  - `rpki::myrpki::EntityDB`, 279
  - `rpki::myrpki::IRDB`, 280
  - `rpki::myrpki::main`, 283
  - `rpki::myrpki::parent`, 292
  - `rpki::myrpki::repository`, 296
  - `rpki::myrpki::roa_request`, 298
  - `rpki::pubd::main`, 302
  - `rpki::resource_set::resource_bag`, 326
  - `rpki::resource_set::resource_range`, 330
  - `rpki::resource_set::resource_set`, 338
  - `rpki::resource_set::roa_prefix`, 348
  - `rpki::resource_set::roa_prefix_set`, 352
  - `rpki::roa::ROAIPAddress`, 356
  - `rpki::roa::ROAIPAddresses`, 357
  - `rpki::roa::ROAIPAddressFamilies`, 357
  - `rpki::roa::ROAIPAddressFamily`, 358
  - `rpki::roa::RouteOriginAttestation`, 359
  - `rpki::rootd::main`, 364
  - `rpki::rpkid::child_cert_obj`, 387
  - `rpki::rpkid::ghostbuster_obj`, 391
  - `rpki::rpkid::main`, 396
  - `rpki::rpkid::publication_queue`, 403
  - `rpki::rpkid::revoked_cert_obj`, 405
  - `rpki::rpkid::roa_obj`, 408
  - `rpki::sql::session`, 414
  - `rpki::sql::template`, 423
  - `rpki::up_down::class_elt`, 439

- rpki::up\_down::class\_response\_syntax, 442
- rpki::up\_down::error\_response\_pdu, 445
- rpki::up\_down::multi\_uri, 456
- rpki::x509::DeadDrop, 470
- rpki::x509::DER\_object, 474
- rpki::x509::PEM\_converter, 483
- rpki::xml\_utils::sax\_handler, 515
- \_\_init\_\_.py(3150), 520
- \_\_iter\_\_
- rpki::myrpki::csv\_reader, 275
- \_\_mul\_\_
- rpki::sundial::timedelta, 431
- \_\_ne\_\_
- rpki::resource\_set::resource\_bag, 327
- \_\_neg\_\_
- rpki::sundial::timedelta, 431
- \_\_new\_\_
- rpki::ipaddrs::v4addr, 211
- rpki::ipaddrs::v6addr, 213
- \_\_pos\_\_
- rpki::sundial::timedelta, 432
- \_\_radd\_\_
- rpki::sundial::datetime, 426
- rpki::sundial::timedelta, 432
- \_\_rdiv\_\_
- rpki::sundial::timedelta, 432
- \_\_repr\_\_
- rpki::async::iterator, 145
- rpki::async::timer, 150
- rpki::http::http\_listener, 191
- rpki::http::http\_queue, 196
- rpki::http::http\_request, 199
- rpki::http::http\_response, 201
- rpki::http::http\_stream, 207
- rpki::myrpki::child, 271
- rpki::myrpki::parent, 292
- rpki::myrpki::repository, 296
- rpki::myrpki::roa\_request, 298
- rpki::rpkid::roa\_obj, 408
- \_\_rfloordiv\_\_
- rpki::sundial::timedelta, 432
- \_\_rmul\_\_
- rpki::sundial::timedelta, 432
- \_\_rsub\_\_
- rpki::sundial::datetime, 426
- rpki::sundial::timedelta, 432
- rpki::http::http\_message, 193
- rpki::ipaddrs::v4addr, 211
- rpki::ipaddrs::v6addr, 213
- rpki::myrpki::comma\_set, 274
- rpki::publication::report\_error\_elt, 322
- rpki::resource\_set::resource\_bag, 327
- rpki::resource\_set::resource\_range\_as, 331
- rpki::resource\_set::resource\_range\_ip, 333
- rpki::resource\_set::resource\_set, 338
- rpki::resource\_set::roa\_prefix, 348
- rpki::resource\_set::roa\_prefix\_set, 352
- rpki::sundial::datetime, 426
- rpki::up\_down::message\_pdu, 452
- rpki::up\_down::multi\_uri, 456
- rpki::xml\_utils::base\_elt, 505
- rpki::xml\_utils::msg, 512
- \_\_sub\_\_
- rpki::sundial::datetime, 426
- rpki::sundial::timedelta, 432
- \_\_add\_\_
- rpki::rpkid::publication\_queue, 403
- \_\_bs2long\_\_
- rpki::resource\_set, 97
- \_\_cast\_\_
- rpki::sundial, 104
- \_\_comm\_\_
- rpki::resource\_set::resource\_set, 338
- \_\_exceptions\_enabled\_\_
- rpki::sql::session, 416
- \_\_find\_xia\_uri\_\_
- rpki::x509, 108
- \_\_long2bs\_\_
- rpki::resource\_set, 97
- \_\_prefixlen\_\_
- rpki::resource\_set::resource\_range\_ip, 335
- \_\_raiseExitNow\_\_
- rpki::async, 66
- \_\_regexp\_\_
- rpki::config::parser, 161
- \_\_repl\_\_
- rpki::config::parser, 159

- `_rsplit`
  - `rpki::resource_set`, 97
- `_wrap_execute`
  - `rpki::sql::session`, 414
- `_yes_or_no_prompts`
  - `rpki::cli`, 69
- `activate`
  - `rpki::rpkiid::ca_detail_obj`, 373
- `active_ca_detail`
  - `rpki::rpkiid::ca_obj`, 381
- `add`
  - `rpki::myrpki::child`, 271
  - `rpki::myrpki::children`, 273
  - `rpki::myrpki::parent`, 292
  - `rpki::myrpki::parents`, 294
  - `rpki::myrpki::repositories`, 295
  - `rpki::myrpki::repository`, 296
  - `rpki::myrpki::roa_request`, 298
  - `rpki::myrpki::roa_requests`, 300
- `addr`
  - `rpki::http::http_client`, 189
- `addr_to_string`
  - `rpki::http`, 75
- `address`
  - `rpki::http::http_client`, 189
  - `rpki::roa::ROAIPAddress`, 356
- `addresses`
  - `rpki::roa::ROAIPAddressFamily`, 358
- `addressFamily`
  - `rpki::roa::ROAIPAddressFamily`, 358
- `adns.py(3465)`, 520
- `af`
  - `rpki::adns::dispatcher`, 132
- `afi`
  - `rpki::resource_set::resource_set_ipv4`, 345
  - `rpki::resource_set::resource_set_ipv6`, 346
- `allow_incomplete`
  - `rpki::myrpki`, 90
- `append`
  - `rpki::resource_set::resource_set`, 338
- `argv`
  - `irbe_cli`, 59
- `asID`
  - `rpki::roa::RouteOriginAttestation`, 360
- `asn`
  - `rpki::left_right::list_resources_elt`, 236
  - `rpki::myrpki::roa_request`, 299
  - `rpki::resource_set::resource_bag`, 328
  - `rpki::rpkiid::roa_obj`, 411
- `asns`
  - `rpki::myrpki::child`, 271
- `assert_pristine`
  - `rpki::sql::session`, 414
- `async.py(3793)`, 521
- `asynchat::async_chat`, 110
- `asyncore::dispatcher`, 110
- `attributes`
  - `rpki::left_right::bsc_elt`, 218
  - `rpki::left_right::child_elt`, 223
  - `rpki::left_right::list_ghostbuster_requests_elt`, 230
  - `rpki::left_right::list_published_objects_elt`, 232
  - `rpki::left_right::list_received_resources_elt`, 234
  - `rpki::left_right::list_resources_elt`, 236
  - `rpki::left_right::list_roa_requests_elt`, 238
  - `rpki::left_right::parent_elt`, 243
  - `rpki::left_right::report_error_elt`, 246
  - `rpki::left_right::repository_elt`, 249
  - `rpki::left_right::self_elt`, 257
  - `rpki::publication::client_elt`, 307
  - `rpki::publication::config_elt`, 311
  - `rpki::publication::publication_object_elt`, 320
  - `rpki::publication::report_error_elt`, 322
  - `rpki::xml_utils::base_elt`, 506
- `b`
  - `rpki::x509::PEM_converter`, 484
- `b64_equal`
  - `rpki::myrpki`, 89
- `backoff`
  - `rpki::adns::query`, 138
- `base64_with_linebreaks`
  - `rpki::x509`, 108
- `base_uri`
  - `rpki::publication::client_elt`, 307

- bits
  - rpki::ipaddr::v4addr, 212
  - rpki::ipaddr::v6addr, 214
- body
  - rpki::http::http\_message, 195
- booleans
  - rpki::left\_right::bsc\_elt, 219
  - rpki::left\_right::child\_elt, 223
  - rpki::left\_right::parent\_elt, 243
  - rpki::left\_right::self\_elt, 257
  - rpki::xml\_utils::base\_elt, 506
- bpki\_cert
  - irbe\_cli::cmd\_elt\_mixin, 115
  - rpki::left\_right::child\_elt, 223
  - rpki::left\_right::repository\_elt, 249
  - rpki::left\_right::self\_elt, 258
  - rpki::publication::client\_elt, 307
- bpki\_certificate
  - rpki::myrpki::child, 271
  - rpki::myrpki::repository, 297
- bpki\_cms\_cert
  - irbe\_cli::cmd\_elt\_mixin, 115
  - rpki::left\_right::parent\_elt, 243
- bpki\_cms\_certificate
  - rpki::myrpki::parent, 292
- bpki\_cms\_glue
  - irbe\_cli::cmd\_elt\_mixin, 116
  - rpki::left\_right::parent\_elt, 243
- bpki\_crl
  - irbe\_cli::config\_elt, 118
- bpki\_glue
  - irbe\_cli::cmd\_elt\_mixin, 116
  - rpki::left\_right::child\_elt, 223
  - rpki::left\_right::repository\_elt, 249
  - rpki::left\_right::self\_elt, 258
  - rpki::publication::client\_elt, 307
- bpki\_resources
  - rpki::myrpki::main, 289
- bpki\_servers
  - rpki::myrpki::main, 289
- bpki\_ta
  - rpki::irdbd::main, 215
  - rpki::pubd::main, 303
  - rpki::rootd::main, 365
  - rpki::rpkid::main, 399
- bsc
  - rpki::left\_right::data\_elt, 226
  - rpki::myrpki::CA, 265
- bscs
  - rpki::left\_right::self\_elt, 253
- buffer
  - rpki::http::http\_stream, 210
- bufsize
  - rpki::adns::dispatcher, 132
- build
  - rpki::x509::Ghostbuster, 481
  - rpki::x509::ROA, 488
  - rpki::x509::SignedManifest, 495
- ca
  - rpki::rpkid::ca\_detail\_obj, 373
- ca\_cert\_uri
  - rpki::rpkid::ca\_detail\_obj, 378
- ca\_detail
  - rpki::rpkid::child\_cert\_obj, 387
  - rpki::rpkid::ghostbuster\_obj, 391
  - rpki::rpkid::revoked\_cert\_obj, 405
  - rpki::rpkid::roa\_obj, 408
- ca\_detail\_id
  - rpki::rpkid::child\_cert\_obj, 389
  - rpki::rpkid::ghostbuster\_obj, 394
  - rpki::rpkid::revoked\_cert\_obj, 406
  - rpki::rpkid::roa\_obj, 411
- ca\_details
  - rpki::rpkid::ca\_obj, 381
- ca\_from\_class\_name
  - rpki::left\_right::child\_elt, 221
- ca\_id
  - rpki::rpkid::ca\_detail\_obj, 378
- cache
  - rpki::sql::session, 416
- cache\_clear
  - rpki::sql::session, 414
- calculate\_SKI
  - rpki::x509, 108
- call\_pubd
  - rpki::left\_right::repository\_elt, 248
  - rpki::rpkid::publication\_queue, 403
- callback
  - rpki::http::http\_request, 200
- caller\_function
  - rpki::async::iterator, 146

- cancel
  - rpki::async::timer, 150
- canonical
  - rpki::resource\_set::resource\_set, 341
- canonize
  - rpki::resource\_set::resource\_set, 338
- cas
  - rpki::left\_right::parent\_elt, 241
- cb
  - rpki::adns::dispatcher, 132
  - rpki::adns::getaddrinfo, 134
  - rpki::adns::query, 138
  - rpki::async::sync\_wrapper, 148
- cer
  - rpki::myrpki::CA, 268
- cert
  - rpki::rpkid::child\_cert\_obj, 389
  - rpki::rpkid::ghostbuster\_obj, 394
  - rpki::rpkid::roa\_obj, 411
  - rpki::up\_down::certificate\_elt, 437
- cert\_url
  - rpki::up\_down::certificate\_elt, 437
  - rpki::up\_down::class\_elt, 440
- certs
  - rpki::up\_down::class\_elt, 440
- cfg
  - irbe\_cli, 59
  - rpki::config::parser, 161
  - rpki::irdbd::main, 215
  - rpki::myrpki::CA, 268
  - rpki::myrpki::main, 289
  - rpki::pubd::main, 303
  - rpki::rootd::main, 365
  - rpki::rpkid::main, 399
- cfg\_file
  - irbe\_cli, 59
  - rpki::myrpki::main, 289
  - rpki::pubd::main, 303
  - rpki::rootd::main, 365
  - rpki::rpkid::main, 399
- characters
  - rpki::xml\_utils::sax\_handler, 515
- check
  - rpki::x509::DER\_object, 474
- check\_allowed\_uri
  - rpki::publication::client\_elt, 306
- check\_auto\_update
  - rpki::x509::DER\_object, 474
- check\_for\_updates
  - rpki::rpkid::ca\_obj, 381
- check\_response
  - rpki::up\_down::base\_elt, 434
  - rpki::up\_down::error\_response\_pdu, 445
  - rpki::up\_down::issue\_response\_pdu, 450
- check\_valid\_rpki
  - rpki::x509::PKCS10, 485
- checkpoint
  - rpki::rpkid::main, 397
- child
  - rpki::rpkid::child\_cert\_obj, 387
- child\_bpki\_cert
  - rpki::rootd::main, 366
- child\_certs
  - rpki::left\_right::child\_elt, 221
  - rpki::rpkid::ca\_detail\_obj, 373
- child\_id
  - rpki::rpkid::child\_cert\_obj, 389
- children
  - rpki::left\_right::bsc\_elt, 218
  - rpki::left\_right::self\_elt, 253
- chop\_into\_prefixes
  - rpki::resource\_set::resource\_range\_ip, 333
- chunk\_body
  - rpki::http::http\_stream, 207
- chunk\_discard\_crlf
  - rpki::http::http\_stream, 207
- chunk\_discard\_trailer
  - rpki::http::http\_stream, 207
- chunk\_handler
  - rpki::http::http\_stream, 210
- chunk\_header
  - rpki::http::http\_stream, 207
- class\_name
  - rpki::up\_down::class\_elt, 440
  - rpki::up\_down::issue\_pdu, 448
  - rpki::up\_down::revoke\_pdu, 458
  - rpki::up\_down::revoke\_syntax, 460
- classes
  - rpki::up\_down::class\_response\_syntax, 443
- cleanup

- rpki::adns::query, 136
- clear
  - rpki::async::timer, 151
  - rpki::x509::DER\_object, 474
- cli.py(3255), 521
- client
  - rpki::http, 75
  - rpki::http::http\_queue, 198
- client\_cert
  - irbe\_cli, 59
  - rpki::http::caller, 184
- client\_getopt
  - irbe\_cli::cmd\_elt\_mixin, 114
- client\_handler
  - rpki::pubd::main, 302
- client\_key
  - irbe\_cli, 60
  - rpki::http::caller, 184
- client\_poll
  - rpki::left\_right::self\_elt, 253
- client\_query\_bpki\_cert
  - irbe\_cli::cmd\_elt\_mixin, 114
- client\_query\_bpki\_cms\_cert
  - irbe\_cli::cmd\_elt\_mixin, 115
- client\_query\_bpki\_crl
  - irbe\_cli::config\_elt, 118
- client\_query\_cms\_glue
  - irbe\_cli::cmd\_elt\_mixin, 115
- client\_query\_glue
  - irbe\_cli::cmd\_elt\_mixin, 115
- client\_query\_signing\_cert
  - irbe\_cli::bsc\_elt, 111
- client\_query\_signing\_cert\_crl
  - irbe\_cli::bsc\_elt, 111
- client\_queues
  - rpki::http, 76
- client\_reply\_decode
  - irbe\_cli::bsc\_elt, 112
  - irbe\_cli::reply\_elt\_mixin, 127
- client\_reply\_show
  - irbe\_cli::reply\_elt\_mixin, 127
- client\_url\_regexp
  - rpki::pubd::main, 303
- close
  - rpki::myrpki::csv\_writer, 277
  - rpki::myrpki::IRDB, 281
  - rpki::sql::session, 415
- cmd
  - rpki::http::http\_request, 200
- cmd::Cmd, 110
- cmdloop\_with\_history
  - rpki::cli::Cmd, 155, 157
- cms\_msg
  - irbe\_cli::left\_right\_proto, 120
  - irbe\_cli::publication\_proto, 125
- cms\_xml\_sign
  - rpki::myrpki::CA, 265
- cms\_xml\_verify
  - rpki::myrpki::CA, 265
- code
  - rpki::http::http\_response, 202
- codes
  - rpki::up\_down::error\_response\_pdu, 446
- collect\_incoming\_data
  - rpki::http::http\_stream, 207
- columns
  - rpki::myrpki::csv\_reader, 276
  - rpki::sql::template, 424
- comment\_characters
  - rpki::myrpki::csv\_reader, 276
- complete\_delete\_child
  - rpki::myrpki::main, 283
- complete\_delete\_parent
  - rpki::myrpki::main, 283
- complete\_delete\_publication\_client
  - rpki::myrpki::main, 283
- complete\_delete\_repository
  - rpki::myrpki::main, 284
- complete\_help
  - rpki::cli::Cmd, 155
- complete\_renew\_child
  - rpki::myrpki::main, 284
- completedefault
  - rpki::myrpki::main, 289
- completenames
  - rpki::cli::Cmd, 155
- compose\_response
  - rpki::rootd::main, 364
- config.py(3620), 522
- config\_id
  - rpki::publication::config\_elt, 311
- configure\_resources\_main

- rpki::myrpki::main, 284
- connect
  - rpki::sql::session, 415
- construct\_sia\_uri
  - rpki::rpkid::ca\_obj, 382
- contains
  - rpki::resource\_set::resource\_set, 339
- content
  - rpki::x509::CMS\_object, 464
  - rpki::x509::DER\_CMS\_object, 472
  - rpki::x509::Ghostbuster, 482
  - rpki::x509::XML\_CMS\_object, 503
- content\_class
  - rpki::x509::ROA, 488
  - rpki::x509::SignedManifest, 495
- control\_handler
  - rpki::pubd::main, 302
- convert\_to\_seconds
  - rpki::sundial::timedelta, 433
- create
  - rpki::rpkid::ca\_detail\_obj, 373
  - rpki::rpkid::ca\_obj, 382
  - rpki::x509::PKCS10, 485
- create\_ca
  - rpki::x509::PKCS10, 485
- create\_top\_level
  - rpki::xml\_utils::sax\_handler, 515
- crl
  - rpki::myrpki::CA, 268
- crl\_interval
  - rpki::left\_right::self\_elt, 258
- crl\_published
  - rpki::rpkid::ca\_detail\_obj, 378
- crl\_published\_callback
  - rpki::rpkid::ca\_detail\_obj, 373
- crl\_uri
  - rpki::rpkid::ca\_detail\_obj, 373
- crl\_uri\_tail
  - rpki::rpkid::ca\_detail\_obj, 374
- crlnum
  - rpki::myrpki::CA, 268
- cron
  - rpki::left\_right::self\_elt, 253
  - rpki::rpkid::main, 397
- cron\_keepalive
  - rpki::rpkid::main, 399
- cron\_period
  - rpki::rpkid::main, 399
- cron\_timeout
  - rpki::rpkid::main, 399
- cron\_timer
  - rpki::rpkid::main, 399
- cronjob\_handler
  - rpki::rpkid::main, 397
- cross\_certify
  - rpki::x509::X509, 497
- cur
  - rpki::irdbd::main, 216
  - rpki::sql::session, 416
- database
  - rpki::sql::session, 416
- datum\_type
  - rpki::resource\_set::resource\_range\_as, 332
  - rpki::resource\_set::resource\_range\_ipv4, 336
  - rpki::resource\_set::resource\_range\_ipv6, 336
- db
  - rpki::irdbd::main, 216
  - rpki::myrpki::IRDB, 281
  - rpki::sql::session, 416
- debug
  - irbe\_cli, 60
  - rpki::http::caller, 184
  - rpki::log, 85
- debug\_cms\_certs
  - rpki::x509::CMS\_object, 464
- debug\_http
  - rpki::http, 76
- decode
  - rpki::x509::DER\_CMS\_object, 472
  - rpki::x509::Ghostbuster, 481
  - rpki::x509::XML\_CMS\_object, 501
- default\_client\_timeout
  - rpki::http, 76
- default\_dirname
  - rpki::config, 70
- default\_envname
  - rpki::config, 70
- default\_filename



- rpki::config, 70
- default\_http\_version
  - rpki::http, 77
- default\_pubd\_handler
  - rpki::left\_right::repository\_elt, 248
- default\_repository
  - rpki::myrpki::main, 289
- default\_section
  - rpki::config::parser, 161
- default\_server\_timeout
  - rpki::http, 77
- default\_tcp\_port
  - rpki::http, 77
- defer
  - rpki::async, 66
- deferred\_queue
  - rpki::async, 67
- del\_subject\_cert
  - rpki::rootd::main, 364
- del\_subject\_pkcs10
  - rpki::rootd::main, 364
- delete
  - rpki::rpkid::ca\_detail\_obj, 374
  - rpki::rpkid::ca\_obj, 382
  - rpki::sql::template, 424
- deprecated\_ca\_details
  - rpki::rpkid::ca\_obj, 382
- DER
  - rpki::x509::CMS\_object, 464
  - rpki::x509::CRL, 469
  - rpki::x509::DER\_object, 479
  - rpki::x509::PKCS10, 486
  - rpki::x509::RSA, 491
  - rpki::x509::RSAPublic, 493
  - rpki::x509::X509, 500
- description
  - rpki::up\_down::error\_response\_pdu, 446
- detach
  - rpki::http::http\_queue, 196
- dict, 110
- difference
  - rpki::resource\_set::resource\_set, 339
- dir
  - rpki::myrpki::CA, 268
  - rpki::myrpki::EntityDB, 279
- dirty
  - rpki::sql::session, 417
- dns\_error
  - rpki::http::http\_client, 187
- do\_configure\_child
  - rpki::myrpki::main, 284
- do\_configure\_daemons
  - rpki::myrpki::main, 284
- do\_configure\_parent
  - rpki::myrpki::main, 285
- do\_configure\_publication\_client
  - rpki::myrpki::main, 285
- do\_configure\_repository
  - rpki::myrpki::main, 286
- do\_configure\_resources
  - rpki::myrpki::main, 286
- do\_delete\_child
  - rpki::myrpki::main, 286
- do\_delete\_parent
  - rpki::myrpki::main, 286
- do\_delete\_publication\_client
  - rpki::myrpki::main, 286
- do\_delete\_repository
  - rpki::myrpki::main, 287
- do\_EOF
  - rpki::cli::Cmd, 155
- do\_exit
  - rpki::cli::Cmd, 155
- do\_initialize
  - rpki::myrpki::main, 287
- do\_quit
  - rpki::cli::Cmd, 157
- do\_renew\_all\_children
  - rpki::myrpki::main, 287
- do\_renew\_child
  - rpki::myrpki::main, 287
- do\_update\_bpki
  - rpki::myrpki::main, 287
- doit
  - rpki::async::iterator, 145
- done
  - rpki::adns::getaddrinfo, 133
  - rpki::adns::test\_getaddrinfo, 140
  - rpki::adns::test\_query, 142
- done1
  - rpki::adns::query, 136
- done2

- rpki::adns::query, [136](#)
- done\_callback
  - rpki::async::iterator, [146](#)
- dump
  - rpki::x509::DeadDrop, [471](#)
- dump\_inbound\_cms
  - rpki::x509::XML\_CMS\_object, [503](#)
- dump\_on\_verify\_failure
  - rpki::x509::CMS\_object, [465](#)
- dump\_outbound\_cms
  - rpki::x509::XML\_CMS\_object, [503](#)
- dump\_to\_disk
  - rpki::x509::XML\_CMS\_object, [502](#)
- dumpasn1
  - rpki::x509::DER\_object, [475](#)
- e
  - rpki::x509::PEM\_converter, [484](#)
- earlier
  - rpki::sundial::datetime, [426](#)
- eb
  - rpki::adns::dispatcher, [132](#)
  - rpki::adns::getaddrinfo, [134](#)
  - rpki::adns::query, [138](#)
  - rpki::async::sync\_wrapper, [148](#)
- eccontent\_oid
  - rpki::x509::CMS\_object, [465](#)
  - rpki::x509::Ghostbuster, [482](#)
  - rpki::x509::ROA, [488](#)
  - rpki::x509::SignedManifest, [495](#)
  - rpki::x509::XML\_CMS\_object, [503](#)
- ee
  - rpki::myrpki::CA, [266](#)
- element\_name
  - rpki::left\_right::bsc\_elt, [219](#)
  - rpki::left\_right::child\_elt, [224](#)
  - rpki::left\_right::list\_ghostbuster\_requests\_ -  
elt, [230](#)
  - rpki::left\_right::list\_published\_objects\_ -  
elt, [232](#)
  - rpki::left\_right::list\_received\_resources\_ -  
elt, [234](#)
  - rpki::left\_right::list\_resources\_elt, [236](#)
  - rpki::left\_right::list\_roa\_requests\_elt, [238](#)
  - rpki::left\_right::parent\_elt, [244](#)
  - rpki::left\_right::report\_error\_elt, [246](#)
  - rpki::left\_right::repository\_elt, [249](#)
  - rpki::left\_right::self\_elt, [258](#)
  - rpki::publication::certificate\_elt, [305](#)
  - rpki::publication::client\_elt, [307](#)
  - rpki::publication::config\_elt, [311](#)
  - rpki::publication::crl\_elt, [313](#)
  - rpki::publication::ghostbuster\_elt, [314](#)
  - rpki::publication::manifest\_elt, [315](#)
  - rpki::publication::report\_error\_elt, [323](#)
  - rpki::publication::roa\_elt, [324](#)
- elements
  - rpki::left\_right::bsc\_elt, [219](#)
  - rpki::left\_right::child\_elt, [224](#)
  - rpki::left\_right::parent\_elt, [244](#)
  - rpki::left\_right::repository\_elt, [249](#)
  - rpki::left\_right::self\_elt, [258](#)
  - rpki::publication::client\_elt, [307](#)
  - rpki::publication::config\_elt, [311](#)
  - rpki::xml\_utils::base\_elt, [507](#)
- empty
  - rpki::resource\_set::resource\_bag, [327](#)
  - rpki::x509::DER\_object, [475](#)
- emptyline
  - rpki::cli::Cmd, [156](#)
- emptyline\_repeats\_last\_command
  - rpki::cli::Cmd, [157](#)
- enable\_ipv6\_clients
  - rpki::http, [77](#)
- enable\_ipv6\_servers
  - rpki::http, [77](#)
- enable\_trace
  - rpki::log, [85](#)
- encode
  - rpki::x509::DER\_CMS\_object, [472](#)
  - rpki::x509::Ghostbuster, [481](#)
  - rpki::x509::XML\_CMS\_object, [502](#)
- encoding
  - rpki::left\_right::cms\_msg, [225](#)
  - rpki::publication::cms\_msg, [308](#)
  - rpki::up\_down::cms\_msg, [443](#)
- endElement
  - rpki::publication::publication\_object\_ -  
elt, [318](#)
  - rpki::up\_down::base\_elt, [435](#)
  - rpki::up\_down::certificate\_elt, [437](#)

- rpki::up\_down::class\_elt, 439
- rpki::up\_down::error\_response\_pdu, 445
- rpki::up\_down::issue\_pdu, 447
- rpki::xml\_utils::base\_elt, 505
- rpki::xml\_utils::data\_elt, 508
- rpki::xml\_utils::msg, 512
- rpki::xml\_utils::sax\_handler, 515
- rpki::xml\_utils::text\_elt, 517
- endElementNS
  - rpki::xml\_utils::sax\_handler, 515
- enforce\_strict\_up\_down\_xml\_sender
  - rpki::left\_right, 82
- entitydb
  - rpki::myrpki::main, 289
- entitydb\_complete
  - rpki::myrpki::main, 288
- env
  - rpki::myrpki::CA, 269
- EOF\_exits\_command\_loop
  - rpki::cli::Cmd, 157
- err
  - rpki::async::sync\_wrapper, 148
- errback
  - rpki::async::timer, 151, 153
  - rpki::http::http\_request, 200
- error
  - rpki::log, 85
- error\_code
  - rpki::left\_right::report\_error\_elt, 246
  - rpki::publication::report\_error\_elt, 323
- error\_text
  - rpki::left\_right::report\_error\_elt, 246
  - rpki::publication::report\_error\_elt, 323
- etree\_post\_read
  - rpki::myrpki, 89
- etree\_pre\_write
  - rpki::myrpki, 89
- etree\_read
  - rpki::myrpki, 89
- etree\_validate
  - rpki::myrpki, 89
- etree\_write
  - rpki::myrpki, 89
- event\_loop
  - rpki::async, 67
- Exception, 111
- exceptions
  - rpki::up\_down::error\_response\_pdu, 446
- exceptions.py(3465), 522
- excludes
  - irbe\_cli::bsc\_elt, 112
  - irbe\_cli::cmd\_elt\_mixin, 116
  - irbe\_cli::list\_published\_objects\_elt, 122
  - irbe\_cli::list\_received\_resources\_elt, 122
- execute
  - rpki::sql::session, 415
- executemany
  - rpki::sql::session, 415
- exit\_event\_loop
  - rpki::async, 67
- ExitNow
  - rpki::async, 67
- expect\_close
  - rpki::http::http\_client, 189
  - rpki::http::http\_server, 205
- expired
  - rpki::x509::X509, 497
- expires
  - rpki::rpkid::revoked\_cert\_obj, 406
- explicitVersion
  - rpki::manifest::Manifest, 263
  - rpki::roa::RouteOriginAttestation, 360
- extend
  - rpki::resource\_set::resource\_set, 339
- extract
  - rpki::x509::CMS\_object, 462
- fetch
  - rpki::publication::config\_elt, 310
  - rpki::rpkid::child\_cert\_obj, 388
- fetch\_child\_certs
  - rpki::left\_right::child\_elt, 222
  - rpki::rpkid::ca\_detail\_obj, 374
- fetchall
  - rpki::sql::session, 415
- file
  - rpki::manifest::FileAndHash, 261
  - rpki::myrpki::csv\_reader, 276
  - rpki::myrpki::csv\_writer, 278
- fileHashAlg
  - rpki::manifest::Manifest, 263
- fileList

- rpki::manifest::Manifest, 263
- filename
  - rpki::config::parser, 161
  - rpki::myrpki::csv\_reader, 276
  - rpki::myrpki::csv\_writer, 278
  - rpki::x509::DER\_object, 479
- filename\_complete
  - rpki::cli::Cmd, 156
- find\_handler
  - rpki::http::http\_server, 203
- format
  - rpki::http::http\_message, 193
- format\_first\_line
  - rpki::http::http\_request, 199
  - rpki::http::http\_response, 201
- formats
  - rpki::x509::CMS\_object, 465
  - rpki::x509::CRL, 469
  - rpki::x509::DER\_object, 479
  - rpki::x509::PKCS10, 486
  - rpki::x509::RSA, 491
  - rpki::x509::RSAPublic, 493
  - rpki::x509::X509, 500
- found\_terminator
  - rpki::http::http\_stream, 208
- from\_bytes
  - rpki::ipaddr::v4addr, 211
  - rpki::ipaddr::v6addr, 213
- from\_csv
  - rpki::myrpki::roa\_requests, 300
- from\_entitydb
  - rpki::myrpki::children, 273
  - rpki::myrpki::parents, 294
  - rpki::myrpki::repositories, 295
- from\_exception
  - rpki::left\_right::report\_error\_elt, 245
  - rpki::publication::report\_error\_elt, 322
- from\_inheritance
  - rpki::resource\_set::resource\_bag, 327
- from\_resource\_bag
  - rpki::up\_down::class\_elt, 439
- from\_rfc3779\_tuples
  - rpki::resource\_set::resource\_bag, 327
- from\_roa\_tuple
  - rpki::resource\_set::roa\_prefix, 348
- from\_sql
  - rpki::resource\_set::resource\_set, 339
  - rpki::resource\_set::roa\_prefix\_set, 352
  - rpki::sundial::datetime, 427
  - rpki::x509::DER\_object, 475
- from\_strings
  - rpki::resource\_set::resource\_range\_as, 331
  - rpki::resource\_set::resource\_range\_ip, 334
- fromASN1tuple
  - rpki::sundial::datetime, 427
- fromdatetime
  - rpki::sundial::datetime, 427
- fromGeneralizedTime
  - rpki::sundial::datetime, 427
- fromOpenSSL
  - rpki::sundial::datetime, 427
- fromtimedelta
  - rpki::sundial::timedelta, 433
- fromUTCtime
  - rpki::sundial::datetime, 427
- fromXMLtime
  - rpki::sundial::datetime, 428
- func
  - rpki::async::sync\_wrapper, 148
- fxcert
  - rpki::myrpki::CA, 266
- gAKI
  - rpki::x509::DER\_object, 475
- gc\_debug
  - rpki::async::timer, 153
- getx
  - rpki::rpkid::ca\_detail\_obj, 378
  - rpki::rpkid::ca\_obj, 385
  - rpki::rpkid::child\_cert\_obj, 389
  - rpki::rpkid::ghostbuster\_obj, 394
  - rpki::rpkid::revoked\_cert\_obj, 406
  - rpki::rpkid::roa\_obj, 412
  - rpki::sql::sql\_persistent, 422
- generate
  - rpki::rpkid::ghostbuster\_obj, 391
  - rpki::rpkid::roa\_obj, 408
  - rpki::x509::CRL, 467
  - rpki::x509::RSA, 490
- generate\_crl

- rpki::rpkid::ca\_detail\_obj, 374
- generate\_manifest
  - rpki::rpkid::ca\_detail\_obj, 374
- generate\_manifest\_cert
  - rpki::rpkid::ca\_detail\_obj, 375
- get
  - rpki::config::parser, 159
- get\_3779resources
  - rpki::x509::DER\_object, 475
- get\_AIA
  - rpki::x509::DER\_object, 476
- get\_aia\_uri
  - rpki::x509::DER\_object, 476
- get\_AKI
  - rpki::x509::DER\_object, 476
- get\_Base64
  - rpki::x509::DER\_object, 476
- get\_basicConstraints
  - rpki::x509::DER\_object, 476
- get\_buffer
  - rpki::http::http\_stream, 208
- get\_content
  - rpki::x509::CMS\_object, 463
- get\_DER
  - rpki::x509::CMS\_object, 463
  - rpki::x509::CRL, 467
  - rpki::x509::DER\_object, 477
  - rpki::x509::PKCS10, 486
  - rpki::x509::RSA, 490
  - rpki::x509::RSAPublic, 492
  - rpki::x509::X509, 497
- get\_PEM
  - rpki::x509::DER\_object, 477
- get\_POW
  - rpki::x509::CMS\_object, 463
  - rpki::x509::CRL, 468
  - rpki::x509::RSA, 490
  - rpki::x509::RSAPublic, 493
  - rpki::x509::X509, 498
- get\_POWpkix
  - rpki::x509::CRL, 468
  - rpki::x509::PKCS10, 486
  - rpki::x509::X509, 498
- get\_public\_DER
  - rpki::x509::RSA, 490
- get\_root\_cert
  - rpki::rootd::main, 364
- get\_RSAPublic
  - rpki::x509::RSA, 490
- get\_SIA
  - rpki::x509::DER\_object, 477
- get\_sia\_directory\_uri
  - rpki::x509::DER\_object, 477
- get\_sia\_manifest\_uri
  - rpki::x509::DER\_object, 477
- get\_signingTime
  - rpki::x509::CMS\_object, 463
- get\_SKI
  - rpki::up\_down::revoke\_pdu, 457
  - rpki::x509::DER\_object, 478
  - rpki::x509::RSA, 490
  - rpki::x509::RSAPublic, 493
- get\_subject\_cert
  - rpki::rootd::main, 364
- get\_subject\_pkcs10
  - rpki::rootd::main, 364
- getboolean
  - rpki::config::parser, 159
- getint
  - rpki::config::parser, 159
- getIssuer
  - rpki::x509::CRL, 468
  - rpki::x509::X509, 498
- getlong
  - rpki::config::parser, 160
- getNextUpdate
  - rpki::x509::CRL, 468
  - rpki::x509::SignedManifest, 495
- getNotAfter
  - rpki::x509::X509, 498
- getNotBefore
  - rpki::x509::X509, 498
- getPublicKey
  - rpki::x509::PKCS10, 486
  - rpki::x509::X509, 498
- getSerial
  - rpki::x509::X509, 499
- getSubject
  - rpki::x509::X509, 499
- getThisUpdate
  - rpki::x509::CRL, 468
  - rpki::x509::SignedManifest, 495

- ghostbuster
  - rpki::rpkid::ghostbuster\_obj, 394
- ghostbusters
  - rpki::left\_right::self\_elt, 253
  - rpki::rpkid::ca\_detail\_obj, 375
- go
  - rpki::adns::query, 136
- gotaddrinfo
  - rpki::http::http\_client, 187
- group
  - rpki::myrpki::roa\_request, 299
- gSKI
  - rpki::x509::DER\_object, 478
- hAKI
  - rpki::x509::DER\_object, 478
- handle
  - rpki::myrpki::child, 272
  - rpki::myrpki::main, 289
  - rpki::myrpki::parent, 292
  - rpki::myrpki::repository, 297
- handle\_accept
  - rpki::http::http\_listener, 191
- handle\_body
  - rpki::http::http\_stream, 208
- handle\_close
  - rpki::http::http\_client, 187
  - rpki::http::http\_stream, 208
- handle\_connect
  - rpki::adns::dispatcher, 131
  - rpki::http::http\_client, 187
- handle\_dispatch
  - rpki::irdbd::main, 216
- handle\_error
  - rpki::adns::dispatcher, 131
  - rpki::http::http\_client, 187
  - rpki::http::http\_listener, 192
  - rpki::http::http\_stream, 209
- handle\_list\_ghostbuster\_requests
  - rpki::irdbd::main, 215
- handle\_list\_resources
  - rpki::irdbd::main, 215
- handle\_list\_roa\_requests
  - rpki::irdbd::main, 215
- handle\_message
  - rpki::http::http\_client, 188
  - rpki::http::http\_server, 203
- handle\_no\_content\_length
  - rpki::http::http\_client, 188
  - rpki::http::http\_server, 204
- handle\_read
  - rpki::adns::dispatcher, 131
- handle\_timeout
  - rpki::http::http\_client, 188
  - rpki::http::http\_stream, 209
- handler
  - rpki::async::gc\_summary, 143
  - rpki::async::timer, 151, 153
  - rpki::irdbd::main, 215
- handler\_common
  - rpki::pubd::main, 302
- handlers
  - rpki::http::http\_listener, 192
  - rpki::http::http\_server, 205
  - rpki::rpkid::publication\_queue, 403
- handles
  - rpki::left\_right::bsc\_elt, 219
  - rpki::left\_right::child\_elt, 224
  - rpki::left\_right::data\_elt, 228
  - rpki::left\_right::parent\_elt, 244
  - rpki::left\_right::repository\_elt, 249
  - rpki::left\_right::self\_elt, 258
- has\_expired
  - rpki::rpkid::ca\_detail\_obj, 375
- has\_option
  - rpki::config::parser, 160
- has\_section
  - rpki::config::parser, 160
- hash
  - rpki::manifest::FileAndHash, 261
- have\_ipv6
  - rpki::http, 78
- have\_readline
  - rpki::cli, 69
- headers
  - rpki::http::http\_message, 195
- help\_help
  - rpki::cli::Cmd, 156
- help\_overview
  - rpki::myrpki::main, 288
- histfile
  - rpki::cli::Cmd, 157

- rpki::myrpki::main, 290
- host
  - rpki::adns::getaddrinfo, 134
  - rpki::http::http\_client, 189
- hostport
  - rpki::http::http\_queue, 198
- hSKI
  - rpki::x509::DER\_object, 478
- http.py(3793), 524
- http\_server\_host
  - rpki::pubd::main, 303
  - rpki::rootd::main, 366
  - rpki::rpkid::main, 400
- http\_server\_port
  - rpki::pubd::main, 303
  - rpki::rootd::main, 366
  - rpki::rpkid::main, 400
- identchars
  - rpki::cli::Cmd, 157
- identity
  - rpki::myrpki::EntityDB, 279
- index
  - rpki::myrpki::CA, 269
  - rpki::sql::template, 424
- info
  - rpki::log, 85
- inherit
  - rpki::resource\_set::resource\_set, 341
  - rpki::resource\_set::resource\_set\_as, 342
  - rpki::resource\_set::resource\_set\_ip, 344
- inherit\_token
  - rpki::resource\_set, 98
- init
  - rpki::log, 84
- initial\_delay
  - rpki::rpkid::main, 400
- insert
  - rpki::sql::template, 424
- intersection
  - rpki::resource\_set::resource\_bag, 327
  - rpki::resource\_set::resource\_set, 339
- interval
  - rpki::async::gc\_summary, 144
- ipAddrBlocks
  - rpki::roa::RouteOriginAttestation, 360
- ipaddrs.py(3551), 526
- ipv4
  - rpki::left\_right::list\_resources\_elt, 236
  - rpki::left\_right::list\_roa\_requests\_elt, 238
  - rpki::rpkid::roa\_obj, 412
- ipv6
  - rpki::left\_right::list\_resources\_elt, 236
  - rpki::left\_right::list\_roa\_requests\_elt, 238
  - rpki::rpkid::roa\_obj, 412
- irbe\_cert
  - rpki::pubd::main, 303
  - rpki::rpkid::main, 400
- irbe\_cli, 57
  - argv, 59
  - cfg, 59
  - cfg\_file, 59
  - client\_cert, 59
  - client\_key, 60
  - debug, 60
  - pem\_out, 60
  - proto, 60
  - q\_msg, 60
  - q\_msg\_left\_right, 60
  - q\_msg\_publication, 60
  - q\_pdu, 61
  - server\_cert, 61
  - server\_ta, 61
  - top\_opts, 61
  - url, 61
  - usage, 59
  - usage\_fill, 61
  - verbose, 61
- irbe\_cli.py(3711), 526
- irbe\_cli::bsc\_elt, 111
  - client\_query\_signing\_cert, 111
  - client\_query\_signing\_cert\_crl, 111
  - client\_reply\_decode, 112
  - excludes, 112
  - signing\_cert, 112
  - signing\_cert\_crl, 112
- irbe\_cli::certificate\_elt, 113
- irbe\_cli::child\_elt, 113
- irbe\_cli::client\_elt, 113
- irbe\_cli::cmd\_elt\_mixin, 114

- bpki\_cert, 115
- bpki\_cms\_cert, 115
- bpki\_cms\_glue, 116
- bpki\_glue, 116
- client\_getopt, 114
- client\_query\_bpki\_cert, 114
- client\_query\_bpki\_cms\_cert, 115
- client\_query\_cms\_glue, 115
- client\_query\_glue, 115
- excludes, 116
- is\_cmd, 116
- usage, 115
- irbe\_cli::cmd\_msg\_mixin, 116
  - usage, 117
- irbe\_cli::config\_elt, 117
  - bpki\_crl, 118
  - client\_query\_bpki\_crl, 118
- irbe\_cli::crl\_elt, 118
- irbe\_cli::left\_right\_cms\_msg, 118
  - saxify, 119
- irbe\_cli::left\_right\_msg, 119
  - pdus, 119
- irbe\_cli::left\_right\_proto, 120
  - cms\_msg, 120
  - msg, 120
- irbe\_cli::left\_right\_sax\_handler, 121
  - pdu, 121
- irbe\_cli::list\_published\_objects\_elt, 121
  - excludes, 122
- irbe\_cli::list\_received\_resources\_elt, 122
  - excludes, 122
- irbe\_cli::manifest\_elt, 123
- irbe\_cli::parent\_elt, 123
- irbe\_cli::publication\_cms\_msg, 123
  - saxify, 124
- irbe\_cli::publication\_msg, 124
  - pdus, 124
- irbe\_cli::publication\_proto, 125
  - cms\_msg, 125
  - msg, 125
- irbe\_cli::publication\_sax\_handler, 126
  - pdu, 126
- irbe\_cli::reply\_elt\_mixin, 126
  - client\_reply\_decode, 127
  - client\_reply\_show, 127
  - is\_cmd, 127
- irbe\_cli::report\_error\_elt, 127
- irbe\_cli::repository\_elt, 128
- irbe\_cli::roa\_elt, 128
- irbe\_cli::self\_elt, 128
- irbe\_cli::UsageWrapper, 129
  - \_\_call\_\_, 129
- irdb\_cert
  - rpki::rpkid::main, 400
- irdb\_query
  - rpki::rpkid::main, 397
- irdb\_query\_child\_resources
  - rpki::rpkid::main, 397
- irdb\_query\_ghostbuster\_requests
  - rpki::rpkid::main, 398
- irdb\_query\_roa\_requests
  - rpki::rpkid::main, 398
- irdb\_url
  - rpki::rpkid::main, 400
- irdbd, 62
- irdbd.py(3569), 528
- irdbd.py(3793), 528
- irdbd\_cert
  - rpki::irdbd::main, 216
- irdbd\_key
  - rpki::irdbd::main, 216
- is\_CA
  - rpki::x509::DER\_object, 478
- is\_cmd
  - irbe\_cli::cmd\_elt\_mixin, 116
  - irbe\_cli::reply\_elt\_mixin, 127
- is\_query
  - rpki::xml\_utils::msg, 512
- is\_reply
  - rpki::xml\_utils::msg, 512
- is\_set
  - rpki::async::timer, 151
- issubset
  - rpki::resource\_set::resource\_set, 340
- issue
  - rpki::rpkid::ca\_detail\_obj, 375
  - rpki::x509::X509, 499
- issue\_ee
  - rpki::rpkid::ca\_detail\_obj, 375
- issue\_response\_candidate\_ca\_details
  - rpki::rpkid::ca\_obj, 383
- issue\_subject\_cert\_maybe



- rpki::rootd::main, 365
- issuer
  - rpki::up\_down::class\_elt, 440
- issuperset
  - rpki::resource\_set::resource\_set, 340
- item\_callback
  - rpki::async::iterator, 146
- iterate
  - rpki::myrpki::EntityDB, 279
- iterator
  - rpki::adns::query, 138
  - rpki::async::iterator, 146
- key
  - rpki::myrpki::CA, 269
- last\_crl\_sn
  - rpki::rpkid::ca\_obj, 385
- last\_issued\_sn
  - rpki::rpkid::ca\_obj, 385
- last\_manifest\_sn
  - rpki::rpkid::ca\_obj, 385
- lastrowid
  - rpki::sql::session, 415
- later
  - rpki::sundial::datetime, 428
- latest\_ca\_cert
  - rpki::rpkid::ca\_detail\_obj, 378
- latest\_crl
  - rpki::rpkid::ca\_detail\_obj, 378
- latest\_manifest
  - rpki::rpkid::ca\_detail\_obj, 378
- latest\_manifest\_cert
  - rpki::rpkid::ca\_detail\_obj, 379
- left\_right
  - rpki::relaxng, 95
- left\_right.py(3793), 528
- left\_right\_handler
  - rpki::rpkid::main, 398
- localhost\_addrinfo
  - rpki::http, 75
- log
  - rpki::http::http\_listener, 192
  - rpki::http::http\_queue, 198
  - rpki::http::http\_stream, 210
- log.py(3793), 529
- log\_method
  - rpki::http, 75
- log\_query
  - rpki::rootd::message\_pdu, 369
  - rpki::up\_down::message\_pdu, 452
- log\_repr
  - rpki::log, 84
- long, 129
- looks\_like\_PEM
  - rpki::x509::PEM\_converter, 483
- loop1
  - rpki::adns::query, 137
- loop2
  - rpki::adns::query, 137
- lose
  - rpki::adns::getaddrinfo, 133
  - rpki::adns::query, 137
  - rpki::adns::test\_getaddrinfo, 140
  - rpki::adns::test\_query, 142
- maildir
  - rpki::x509::DeadDrop, 471
- main
  - rpki::pubd::main, 302
  - rpki::rpkid::main, 396
- make\_b64elt
  - rpki::up\_down::base\_elt, 435
  - rpki::xml\_utils::base\_elt, 505
- make\_elt
  - rpki::up\_down::base\_elt, 435
  - rpki::xml\_utils::base\_elt, 505
- make\_pdu
  - rpki::xml\_utils::base\_elt, 505
- make\_prefix
  - rpki::resource\_set::resource\_range\_ip, 334
- make\_publish
  - rpki::publication::publication\_object\_elt, 319
- make\_query
  - rpki::up\_down::message\_pdu, 453
- make\_reply
  - rpki::left\_right::list\_published\_objects\_elt, 231
  - rpki::left\_right::list\_received\_resources\_elt, 233

- rpki::xml\_utils::data\_elt, 508
- make\_reply\_clone\_hook
  - rpki::left\_right::data\_elt, 226
  - rpki::xml\_utils::data\_elt, 508
- make\_withdraw
  - rpki::publication::publication\_object\_elt, 319
- manifest.py(3598), 530
- manifest\_private\_key\_id
  - rpki::rpkid::ca\_detail\_obj, 379
- manifest\_public\_key
  - rpki::rpkid::ca\_detail\_obj, 379
- manifest\_published
  - rpki::rpkid::ca\_detail\_obj, 379
- manifest\_published\_callback
  - rpki::rpkid::ca\_detail\_obj, 376
- manifest\_uri
  - rpki::rpkid::ca\_detail\_obj, 376
- manifestNumber
  - rpki::manifest::Manifest, 263
- map
  - rpki::sql::template, 424
- max
  - rpki::resource\_set::resource\_range, 330
  - rpki::resource\_set::roa\_prefix, 348
- max\_prefixlen
  - rpki::resource\_set::roa\_prefix, 349
- maxLength
  - rpki::roa::ROAIPAddress, 356
- min
  - rpki::resource\_set::resource\_range, 330
  - rpki::resource\_set::resource\_range\_as, 332
  - rpki::resource\_set::roa\_prefix, 348
- min\_columns
  - rpki::myrpki::csv\_reader, 276
- msg
  - irbe\_cli::left\_right\_proto, 120
  - irbe\_cli::publication\_proto, 125
  - rpki::http::http\_stream, 210
- msgs
  - rpki::rpkid::publication\_queue, 403
- multiget
  - rpki::config::parser, 160
- myhandle
  - rpki::myrpki::parent, 293
- myrpki.py(3793), 530
- name
  - rpki::left\_right::sax\_handler, 251
  - rpki::publication::sax\_handler, 325
  - rpki::up\_down::sax\_handler, 460
- name2oid
  - rpki::oids, 92
- name2type
  - rpki::rootd::message\_pdu, 369
  - rpki::up\_down::message\_pdu, 454
- nameservers
  - rpki::adns, 65
  - rpki::adns::query, 138
- namespace
  - rpki::myrpki, 90
- namespaceQName
  - rpki::myrpki, 90
- next\_crl\_number
  - rpki::rpkid::ca\_obj, 383
- next\_manifest\_number
  - rpki::rpkid::ca\_obj, 383
- next\_serial\_number
  - rpki::rpkid::ca\_obj, 383
- nextUpdate
  - rpki::manifest::Manifest, 263
- normalize\_chain
  - rpki::x509::X509, 499
- normalize\_headers
  - rpki::http::http\_message, 194
- note
  - rpki::log, 85
- now
  - rpki::sundial, 104
- nsmap
  - rpki::left\_right::left\_right\_namespace, 229
  - rpki::publication::publication\_namespace, 317
  - rpki::up\_down, 106
- obj
  - rpki::left\_right::list\_published\_objects\_elt, 232
- object, 129
- oid2name

- rpki::oids, [92](#)
- oids.py(3725), [531](#)
- onecmd
  - rpki::cli::Cmd, [156](#)
- openssl
  - rpki::myrpki::CA, [269](#)
- other\_clear
  - rpki::x509::CMS\_object, [465](#)
  - rpki::x509::DER\_object, [480](#)
- oversized
  - rpki::resource\_set::resource\_bag, [328](#)
- parent
  - rpki::rpkid::ca\_obj, [383](#)
- parent\_id
  - rpki::rpkid::ca\_obj, [385](#)
- parent\_resource\_class
  - rpki::rpkid::ca\_obj, [385](#)
- parents
  - rpki::left\_right::bsc\_elt, [218](#)
  - rpki::left\_right::child\_elt, [222](#)
  - rpki::left\_right::repository\_elt, [248](#)
  - rpki::left\_right::self\_elt, [253](#)
- parse
  - rpki::ipaddrs, [80](#)
  - rpki::sundial::timedelta, [433](#)
- parse\_first\_line
  - rpki::http::http\_request, [199](#)
  - rpki::http::http\_response, [202](#)
- parse\_from\_wire
  - rpki::http::http\_message, [194](#)
- parse\_rfc3779\_tuple
  - rpki::resource\_set::resource\_set\_as, [342](#)
  - rpki::resource\_set::resource\_set\_ip, [344](#)
- parse\_str
  - rpki::resource\_set::resource\_range\_as, [332](#)
  - rpki::resource\_set::resource\_range\_ip, [334](#)
  - rpki::resource\_set::resource\_set, [340](#)
  - rpki::resource\_set::roa\_prefix, [349](#)
  - rpki::resource\_set::roa\_prefix\_set, [353](#)
- parse\_type
  - rpki::http::http\_client, [189](#)
  - rpki::http::http\_server, [205](#)
- parse\_version
  - rpki::http::http\_message, [194](#)
- password
  - rpki::sql::session, [417](#)
- path
  - rpki::http::http\_request, [200](#)
- path\_restriction
  - rpki::myrpki::CA, [269](#)
- payload
  - rpki::publication::publication\_object\_elt, [320](#)
  - rpki::up\_down::message\_pdu, [454](#)
- payload\_type
  - rpki::publication::certificate\_elt, [305](#)
  - rpki::publication::crl\_elt, [313](#)
  - rpki::publication::ghostbuster\_elt, [314](#)
  - rpki::publication::manifest\_elt, [315](#)
  - rpki::publication::publication\_object\_elt, [321](#)
  - rpki::publication::roa\_elt, [324](#)
- pdu
  - irbe\_cli::left\_right\_sax\_handler, [121](#)
  - irbe\_cli::publication\_sax\_handler, [126](#)
  - rpki::left\_right::sax\_handler, [251](#)
  - rpki::publication::sax\_handler, [325](#)
  - rpki::rootd::sax\_handler, [371](#)
  - rpki::up\_down::sax\_handler, [461](#)
- pdus
  - irbe\_cli::left\_right\_msg, [119](#)
  - irbe\_cli::publication\_msg, [124](#)
  - rpki::left\_right::msg, [239](#)
  - rpki::publication::msg, [316](#)
- pem\_converter
  - rpki::x509::CMS\_object, [465](#)
  - rpki::x509::CRL, [469](#)
  - rpki::x509::DER\_object, [480](#)
  - rpki::x509::Ghostbuster, [482](#)
  - rpki::x509::PKCS10, [487](#)
  - rpki::x509::ROA, [488](#)
  - rpki::x509::RSA, [491](#)
  - rpki::x509::RSAPublic, [493](#)
  - rpki::x509::SignedManifest, [495](#)
  - rpki::x509::X509, [500](#)
- pem\_out
  - irbe\_cli, [60](#)
- PEMBase64
  - rpki::myrpki, [90](#)

- PEMElement
  - rpki::myrpki, 90
- pending\_ca\_details
  - rpki::rpkid::ca\_obj, 384
- persistent
  - rpki::http::http\_message, 194
- pid
  - rpki::log, 85
  - rpki::x509::DeadDrop, 471
- ping
  - rpki::sql::session, 415
- pkcs10
  - rpki::up\_down::issue\_pdu, 448
- pkcs10\_request
  - rpki::left\_right::bsc\_elt, 219
- PKIX\_threshold
  - rpki::sundial::datetime, 429
- port
  - rpki::http::http\_client, 190
- POW
  - rpki::x509::CMS\_object, 466
  - rpki::x509::CRL, 469
  - rpki::x509::RSA, 491
  - rpki::x509::RSAPublic, 494
  - rpki::x509::X509, 500
- POWify\_OID
  - rpki::x509, 108
- POWpkix
  - rpki::x509::CRL, 469
  - rpki::x509::PKCS10, 487
  - rpki::x509::X509, 500
- prefix
  - rpki::resource\_set::roa\_prefix, 349
- prefix\_type
  - rpki::resource\_set::roa\_prefix\_set\_ipv4, 354
  - rpki::resource\_set::roa\_prefix\_set\_ipv6, 355
- prefixlen
  - rpki::resource\_set::resource\_range\_ip, 334
  - rpki::resource\_set::roa\_prefix, 350
- pretty\_print\_content
  - rpki::x509::XML\_CMS\_object, 502
- print\_on\_der\_error
  - rpki::x509::CMS\_object, 466
- priority
  - rpki::log::logger, 260
- private\_key\_id
  - rpki::left\_right::bsc\_elt, 219
  - rpki::rpkid::ca\_detail\_obj, 379
- profile
  - rpki::pubd::main, 303
  - rpki::rpkid::main, 400
- prompt
  - rpki::myrpki::main, 290
- proto
  - irbe\_cli, 60
  - rpki::http::caller, 184
- pubd, 62
  - pubd.py(3569), 532
  - pubd.py(3793), 531
- pubd\_cert
  - rpki::pubd::main, 304
- pubd\_contact\_info
  - rpki::myrpki::main, 290
- pubd\_key
  - rpki::pubd::main, 304
- public\_key
  - rpki::rpkid::ca\_detail\_obj, 379
- publication
  - rpki::relaxng, 95
  - publication.py(3793), 532
- publication\_base
  - rpki::pubd::main, 304
- publication\_kludge\_base
  - rpki::rpkid::main, 401
- publication\_multimodule
  - rpki::pubd::main, 304
- publish
  - rpki::rpkid::publication\_queue, 403
- published
  - rpki::rpkid::child\_cert\_obj, 390
  - rpki::rpkid::ghostbuster\_obj, 394
  - rpki::rpkid::roa\_obj, 412
- published\_callback
  - rpki::rpkid::child\_cert\_obj, 388
  - rpki::rpkid::ghostbuster\_obj, 392
  - rpki::rpkid::roa\_obj, 409
- pydatetime::datetime, 130
- pydatetime::timedelta, 130

- q\_msg
  - irbe\_cli, 60
- q\_msg\_left\_right
  - irbe\_cli, 60
- q\_msg\_publication
  - irbe\_cli, 60
- q\_pdu
  - irbe\_cli, 61
- qclass
  - rpki::adns::query, 138
  - rpki::adns::test\_query, 142
- qname
  - rpki::adns::query, 139
  - rpki::adns::test\_getaddrinfo, 141
  - rpki::adns::test\_query, 142
- qtype
  - rpki::adns::query, 139
  - rpki::adns::test\_query, 142
- queries
  - rpki::adns::getaddrinfo, 134
- query
  - rpki::up\_down::issue\_pdu, 447
  - rpki::up\_down::list\_pdu, 450
  - rpki::up\_down::revoke\_pdu, 457
  - rpki::xml\_utils::msg, 512
- query\_up\_down
  - rpki::left\_right::parent\_elt, 241
- queue
  - rpki::async::timer, 153
  - rpki::http::http\_client, 190
  - rpki::http::http\_queue, 198
- raise\_if\_error
  - rpki::publication::publication\_object\_elt, 319
  - rpki::publication::report\_error\_elt, 322
- range\_type
  - rpki::resource\_set::resource\_set\_as, 343
  - rpki::resource\_set::resource\_set\_ipv4, 345
  - rpki::resource\_set::resource\_set\_ipv6, 346
  - rpki::resource\_set::roa\_prefix\_ipv4, 350
  - rpki::resource\_set::roa\_prefix\_ipv6, 351
- re\_address\_range
  - rpki::resource\_set, 98
- re\_asn\_range
  - rpki::resource\_set, 98
- re\_prefix
  - rpki::resource\_set, 99
- re\_prefix\_with\_maxlen
  - rpki::resource\_set, 99
- read\_attrs
  - rpki::xml\_utils::base\_elt, 505
- read\_config
  - rpki::myrpki::main, 288
- reason
  - rpki::http::http\_response, 202
- recipient
  - rpki::up\_down::message\_pdu, 454
- regen\_margin
  - rpki::left\_right::self\_elt, 259
- regenerate
  - rpki::rpkid::ghostbuster\_obj, 392
  - rpki::rpkid::roa\_obj, 409
- regenerate\_crls\_and\_manifests
  - rpki::left\_right::self\_elt, 254
- regexp
  - rpki::sundial::timedelta, 433
- reissue
  - rpki::rpkid::ca\_detail\_obj, 376
  - rpki::rpkid::ca\_obj, 384
  - rpki::rpkid::child\_cert\_obj, 388
- rekey
  - rpki::rpkid::ca\_obj, 384
- relaxng.py(3731), 532
- renew\_children\_common
  - rpki::myrpki::main, 288
- renmwo
  - rpki::myrpki::csv\_writer, 278
- replace
  - rpki::rpkid::publication\_queue, 404
- reply
  - rpki::xml\_utils::msg, 513
- repositories
  - rpki::left\_right::bsc\_elt, 218
  - rpki::left\_right::self\_elt, 254
  - rpki::rpkid::publication\_queue, 404
- repository
  - rpki::left\_right::parent\_elt, 241
- req
  - rpki::myrpki::CA, 269

- req\_resource\_set\_as
  - rpki::up\_down::certificate\_elt, 437
  - rpki::up\_down::issue\_pdu, 449
- req\_resource\_set\_ipv4
  - rpki::up\_down::certificate\_elt, 438
  - rpki::up\_down::issue\_pdu, 449
- req\_resource\_set\_ipv6
  - rpki::up\_down::certificate\_elt, 438
  - rpki::up\_down::issue\_pdu, 449
- request
  - rpki::adns::query, 139
  - rpki::http::http\_queue, 197
- require\_crls
  - rpki::x509::CMS\_object, 466
- res
  - rpki::async::sync\_wrapper, 148
- resolver
  - rpki::adns, 65
- resource\_set.py(3688), 533
- resource\_set\_as
  - rpki::up\_down::class\_elt, 441
- resource\_set\_ipv4
  - rpki::up\_down::class\_elt, 441
- resource\_set\_ipv6
  - rpki::up\_down::class\_elt, 441
- resource\_set\_notafter
  - rpki::up\_down::class\_elt, 441
- resource\_set\_type
  - rpki::resource\_set::roa\_prefix\_set\_ipv4, 354
  - rpki::resource\_set::roa\_prefix\_set\_ipv6, 355
- response
  - rpki::adns::query, 139
- restart
  - rpki::http::http\_queue, 197
  - rpki::http::http\_stream, 209
- result
  - rpki::adns::getaddrinfo, 134
  - rpki::xml\_utils::sax\_handler, 516
- retrieved
  - rpki::http::http\_request, 200
- return\_result
  - rpki::http::http\_queue, 197
- revoke
  - rpki::rpkid::ca\_detail\_obj, 376
  - rpki::rpkid::ca\_obj, 384
  - rpki::rpkid::child\_cert\_obj, 388
  - rpki::rpkid::ghostbuster\_obj, 392
  - rpki::rpkid::revoked\_cert\_obj, 405
  - rpki::rpkid::roa\_obj, 409
- revoked
  - rpki::rpkid::revoked\_cert\_obj, 406
- revoked\_ca\_details
  - rpki::rpkid::ca\_obj, 384
- revoked\_certs
  - rpki::rpkid::ca\_detail\_obj, 377
- roa
  - rpki::rpkid::roa\_obj, 412
- roa.py(3598), 534
- roas
  - rpki::left\_right::self\_elt, 254
  - rpki::rpkid::ca\_detail\_obj, 377
- root\_newer\_than\_subject
  - rpki::rootd::main, 365
- rootd, 63
  - rpki::rootd, 101
- rootd.py(3569), 535
- rootd.py(3793), 534
- rootd\_bpki\_cert
  - rpki::rootd::main, 366
- rootd\_bpki\_crl
  - rpki::rootd::main, 366
- rootd\_bpki\_key
  - rpki::rootd::main, 366
- rpki, 63
  - rpki.\_\_doc\_\_, 64
  - rpki.adns, 64
  - rpki.async, 65
  - rpki.cli, 68
  - rpki.config, 69
  - rpki.exceptions, 71
  - rpki.http, 73
  - rpki.ipaddrs, 79
  - rpki.irdbd, 80
  - rpki.left\_right, 81
  - rpki.log, 82
  - rpki.manifest, 86
  - rpki.myrpki, 87
  - rpki.oids, 91
  - rpki.pubd, 92
  - rpki.publication, 93

- rpki.relaxng, 94
- rpki.resource\_set, 95
- rpki.roa, 99
- rpki.rootd, 100
- rpki.rpkid, 101
- rpki.sql, 102
- rpki.sundial, 103
- rpki.up\_down, 105
- rpki.x509, 106
- rpki.xml\_utils, 109
- rpki::adns
  - nameservers, 65
  - resolver, 65
- rpki::adns::dispatcher, 130
  - \_\_init\_\_, 131
  - af, 132
  - bufsize, 132
  - cb, 132
  - eb, 132
  - handle\_connect, 131
  - handle\_error, 131
  - handle\_read, 131
  - writable, 131
- rpki::adns::getaddrinfo, 132
  - \_\_init\_\_, 133
  - cb, 134
  - done, 133
  - eb, 134
  - host, 134
  - lose, 133
  - queries, 134
  - result, 134
  - typemap, 134
- rpki::adns::query, 135
  - \_\_init\_\_, 136
  - backoff, 138
  - cb, 138
  - cleanup, 136
  - done1, 136
  - done2, 136
  - eb, 138
  - go, 136
  - iterator, 138
  - loop1, 137
  - loop2, 137
  - lose, 137
  - nameservers, 138
  - qclass, 138
  - qname, 139
  - qtype, 139
  - request, 139
  - response, 139
  - socket\_cb, 137
  - socket\_eb, 137
  - socket\_timeout, 138
  - sockets, 139
  - start, 139
  - timer, 139
- rpki::adns::test\_getaddrinfo, 140
  - \_\_init\_\_, 140
  - done, 140
  - lose, 140
  - qname, 141
- rpki::adns::test\_query, 141
  - \_\_init\_\_, 142
  - done, 142
  - lose, 142
  - qclass, 142
  - qname, 142
  - qtype, 142
- rpki::async
  - \_raiseExitNow, 66
  - defer, 66
  - deferred\_queue, 67
  - event\_loop, 67
  - exit\_event\_loop, 67
  - ExitNow, 67
  - run\_deferred, 67
- rpki::async::gc\_summary, 143
  - \_\_init\_\_, 143
  - handler, 143
  - interval, 144
  - threshold, 144
  - timer, 144
- rpki::async::iterator, 144
  - \_\_call\_\_, 145
  - \_\_init\_\_, 145
  - \_\_repr\_\_, 145
  - caller\_function, 146
  - doit, 145
  - done\_callback, 146
  - item\_callback, 146

- iterator, 146
- unwind\_stack, 146
- rpki::async::sync\_wrapper, 146
  - \_\_call\_\_, 147
  - \_\_init\_\_, 147
- cb, 148
- eb, 148
- err, 148
- func, 148
- res, 148
- rpki::async::timer, 149
  - \_\_cmp\_\_, 150
  - \_\_del\_\_, 150
  - \_\_init\_\_, 150
  - \_\_repr\_\_, 150
- cancel, 150
- clear, 151
- errback, 151, 153
- gc\_debug, 153
- handler, 151, 153
- is\_set, 151
- queue, 153
- run\_debug, 153
- runq, 151
- seconds\_until\_wakeup, 152
- set, 152
- set\_errback, 152
- set\_handler, 152
- trace, 153
- when, 153
- rpki::cli
  - \_yes\_or\_no\_prompts, 69
  - have\_readline, 69
  - yes\_or\_no, 68
- rpki::cli::Cmd, 154
  - \_\_init\_\_, 155
  - cmdloop\_with\_history, 155, 157
  - complete\_help, 155
  - completenames, 155
  - do\_EOF, 155
  - do\_exit, 155
  - do\_quit, 157
  - emptyline, 156
  - emptyline\_repeats\_last\_command, 157
  - EOF\_exits\_command\_loop, 157
  - filename\_complete, 156
  - help\_help, 156
  - histfile, 157
  - identchars, 157
  - onecmd, 156
- rpki::config
  - default\_dirname, 70
  - default\_envname, 70
  - default\_filename, 70
- rpki::config::parser, 158
  - \_\_init\_\_, 159
  - \_regexp, 161
  - \_repl, 159
  - cfg, 161
  - default\_section, 161
  - filename, 161
  - get, 159
  - getboolean, 159
  - getint, 159
  - getlong, 160
  - has\_option, 160
  - has\_section, 160
  - multiget, 160
  - set\_global\_flags, 160
- rpki::exceptions::BadClassNameSyntax, 161
- rpki::exceptions::BadClientURL, 162
- rpki::exceptions::BadContactURL, 162
- rpki::exceptions::BadExtension, 163
- rpki::exceptions::BadIPResource, 163
- rpki::exceptions::BadIRDBReply, 163
- rpki::exceptions::BadIssueResponse, 164
- rpki::exceptions::BadPKCS10, 164
- rpki::exceptions::BadPublicationReply, 164
- rpki::exceptions::BadQuery, 165
- rpki::exceptions::BadROAPrefix, 165
- rpki::exceptions::BadSender, 165
- rpki::exceptions::BadStatusCode, 166
- rpki::exceptions::BadURISyntax, 166
- rpki::exceptions::BSCNotFound, 167
- rpki::exceptions::BSCNotReady, 167
- rpki::exceptions::ChildNotFound, 167
- rpki::exceptions::ClassNameMismatch, 168
- rpki::exceptions::ClassNameUnknown, 168
- rpki::exceptions::ClientNotFound, 168
- rpki::exceptions::CMSContentNotSet, 169
- rpki::exceptions::CMSCRLNotSet, 169
- rpki::exceptions::CMSVerificationFailed, 169



- rpki::exceptions::CommandParseFailure, 170
- rpki::exceptions::DBConsistencyError, 170
- rpki::exceptions::DERObjectConversionError, 171
- rpki::exceptions::DuplicateObject, 171
- rpki::exceptions::EmptyPEM, 171
- rpki::exceptions::EmptyROAPrefixList, 172
- rpki::exceptions::ForbiddenURI, 172
- rpki::exceptions::HandleTranslationError, 172
- rpki::exceptions::HTTPBadVersion, 173
- rpki::exceptions::HTTPClientAborted, 173
- rpki::exceptions::HTTPRequestFailed, 173
- rpki::exceptions::HTTPTimeout, 174
- rpki::exceptions::HTTPUnexpectedState, 174
- rpki::exceptions::MissingCMSCRL, 175
- rpki::exceptions::MissingCMSEECert, 175
- rpki::exceptions::MultipleTLSEECert, 175
- rpki::exceptions::MustBePrefix, 176
- rpki::exceptions::NoActiveCA, 176
- rpki::exceptions::NoCoveringCertForROA, 176
- rpki::exceptions::NoObjectAtURI, 177
- rpki::exceptions::NotACertificateChain, 177
- rpki::exceptions::NotFound, 177
- rpki::exceptions::NotImplementedYet, 178
- rpki::exceptions::NotInDatabase, 178
- rpki::exceptions::ReceivedTLSCACert, 179
- rpki::exceptions::RPKI\_Exception, 179
- rpki::exceptions::ServerShuttingDown, 180
- rpki::exceptions::SKIMismatch, 180
- rpki::exceptions::SubprocessError, 180
- rpki::exceptions::TLSValidationError, 181
- rpki::exceptions::UnexpectedCMSCerts, 181
- rpki::exceptions::UnexpectedCMSCRLs, 182
- rpki::exceptions::UnparsableCMSDER, 182
- rpki::exceptions::UpstreamError, 182
- rpki::exceptions::WrongContentType, 183
- rpki::http
  - addr\_to\_string, 75
  - client, 75
  - client\_queues, 76
  - debug\_http, 76
  - default\_client\_timeout, 76
  - default\_http\_version, 77
  - default\_server\_timeout, 77
  - default\_tcp\_port, 77
  - enable\_ipv6\_clients, 77
  - enable\_ipv6\_servers, 77
  - have\_ipv6, 78
  - localhost\_addrinfo, 75
  - log\_method, 75
  - rpki\_content\_type, 78
  - server, 76
  - supported\_address\_families, 76
  - use\_adns, 78
  - want\_persistent\_client, 78
  - want\_persistent\_server, 78
- rpki::http:caller, 183
  - \_\_call\_\_, 184
  - \_\_init\_\_, 184
  - client\_cert, 184
  - client\_key, 184
  - debug, 184
  - proto, 184
  - server\_cert, 185
  - server\_ta, 185
  - url, 185
- rpki::http:http\_client, 185
  - \_\_init\_\_, 186
  - addr, 189
  - address, 189
  - dns\_error, 187
  - expect\_close, 189
  - gotaddrinfo, 187
  - handle\_close, 187
  - handle\_connect, 187
  - handle\_error, 187
  - handle\_message, 188
  - handle\_no\_content\_length, 188
  - handle\_timeout, 188
  - host, 189
  - parse\_type, 189
  - port, 190
  - queue, 190
  - send\_request, 188
  - set\_state, 188
  - start, 189
  - state, 190
  - timeout, 190
- rpki::http:http\_listener, 190
  - \_\_init\_\_, 191

- [\\_\\_repr\\_\\_, 191](#)
  - [handle\\_accept, 191](#)
  - [handle\\_error, 192](#)
  - [handlers, 192](#)
  - [log, 192](#)
  - [show\\_tracebacks, 192](#)
- [rpki::http::http\\_message, 192](#)
  - [\\_\\_init\\_\\_, 193](#)
  - [\\_\\_str\\_\\_, 193](#)
  - [body, 195](#)
  - [format, 193](#)
  - [headers, 195](#)
  - [normalize\\_headers, 194](#)
  - [parse\\_from\\_wire, 194](#)
  - [parse\\_version, 194](#)
  - [persistent, 194](#)
  - [software\\_name, 195](#)
  - [version, 195](#)
- [rpki::http::http\\_queue, 195](#)
  - [\\_\\_init\\_\\_, 196](#)
  - [\\_\\_repr\\_\\_, 196](#)
  - [client, 198](#)
  - [detach, 196](#)
  - [hostport, 198](#)
  - [log, 198](#)
  - [queue, 198](#)
  - [request, 197](#)
  - [restart, 197](#)
  - [return\\_result, 197](#)
  - [send\\_request, 197](#)
- [rpki::http::http\\_request, 198](#)
  - [\\_\\_init\\_\\_, 199](#)
  - [\\_\\_repr\\_\\_, 199](#)
  - [callback, 200](#)
  - [cmd, 200](#)
  - [errback, 200](#)
  - [format\\_first\\_line, 199](#)
  - [parse\\_first\\_line, 199](#)
  - [path, 200](#)
  - [retried, 200](#)
- [rpki::http::http\\_response, 201](#)
  - [\\_\\_init\\_\\_, 201](#)
  - [\\_\\_repr\\_\\_, 201](#)
  - [code, 202](#)
  - [format\\_first\\_line, 201](#)
  - [parse\\_first\\_line, 202](#)
  - [reason, 202](#)
- [rpki::http::http\\_server, 202](#)
  - [\\_\\_init\\_\\_, 203](#)
  - [expect\\_close, 205](#)
  - [find\\_handler, 203](#)
  - [handle\\_message, 203](#)
  - [handle\\_no\\_content\\_length, 204](#)
  - [handlers, 205](#)
  - [parse\\_type, 205](#)
  - [send\\_error, 204](#)
  - [send\\_message, 204](#)
  - [send\\_reply, 204](#)
  - [timeout, 205](#)
- [rpki::http::http\\_stream, 205](#)
  - [\\_\\_init\\_\\_, 206](#)
  - [\\_\\_repr\\_\\_, 207](#)
  - [buffer, 210](#)
  - [chunk\\_body, 207](#)
  - [chunk\\_discard\\_crlf, 207](#)
  - [chunk\\_discard\\_trailer, 207](#)
  - [chunk\\_handler, 210](#)
  - [chunk\\_header, 207](#)
  - [collect\\_incoming\\_data, 207](#)
  - [found\\_terminator, 208](#)
  - [get\\_buffer, 208](#)
  - [handle\\_body, 208](#)
  - [handle\\_close, 208](#)
  - [handle\\_error, 209](#)
  - [handle\\_timeout, 209](#)
  - [log, 210](#)
  - [msg, 210](#)
  - [restart, 209](#)
  - [show\\_tracebacks, 210](#)
  - [timer, 210](#)
  - [update\\_timeout, 209](#)
- [rpki::ipaddrs](#)
  - [parse, 80](#)
- [rpki::ipaddrs::v4addr, 211](#)
  - [\\_\\_new\\_\\_, 211](#)
  - [\\_\\_str\\_\\_, 211](#)
  - [bits, 212](#)
  - [from\\_bytes, 211](#)
  - [to\\_bytes, 212](#)
- [rpki::ipaddrs::v6addr, 212](#)
  - [\\_\\_new\\_\\_, 213](#)
  - [\\_\\_str\\_\\_, 213](#)

- bits, 214
- from\_bytes, 213
- to\_bytes, 213
- rpki::irdbd::main, 214
- \_\_init\_\_, 215
- bpki\_ta, 215
- cfg, 215
- cur, 216
- db, 216
- handle\_dispatch, 216
- handle\_list\_ghostbuster\_requests, 215
- handle\_list\_resources, 215
- handle\_list\_roa\_requests, 215
- handler, 215
- irdbd\_cert, 216
- irdbd\_key, 216
- rpkiid\_cert, 216
- rpki::left\_right
  - enforce\_strict\_up\_down\_xml\_sender, 82
- rpki::left\_right::bsc\_elt, 217
  - attributes, 218
  - booleans, 219
  - children, 218
  - element\_name, 219
  - elements, 219
  - handles, 219
  - parents, 218
  - pkcs10\_request, 219
  - private\_key\_id, 219
  - repositories, 218
  - serve\_pre\_save\_hook, 218
  - signing\_cert, 220
  - signing\_cert\_crl, 220
  - sql\_template, 220
- rpki::left\_right::child\_elt, 220
  - attributes, 223
  - booleans, 223
  - bpki\_cert, 223
  - bpki\_glue, 223
  - ca\_from\_class\_name, 221
  - child\_certs, 221
  - element\_name, 224
  - elements, 224
  - fetch\_child\_certs, 222
  - handles, 224
  - parents, 222
  - serve\_destroy\_hook, 222
  - serve\_post\_save\_hook, 222
  - serve\_reissue, 222
  - serve\_up\_down, 223
  - sql\_template, 224
- rpki::left\_right::cms\_msg, 225
  - encoding, 225
  - saxify, 225
  - schema, 225
- rpki::left\_right::data\_elt, 226
  - bsc, 226
  - handles, 228
  - make\_reply\_clone\_hook, 226
  - self, 227
  - self\_handle, 228
  - self\_id, 228
  - serve\_fetch\_all, 227
  - serve\_fetch\_handle, 227
  - serve\_fetch\_one\_maybe, 227
  - serve\_pre\_save\_hook, 227
- rpki::left\_right::left\_right\_namespace, 228
  - nsmmap, 229
  - xmlns, 229
- rpki::left\_right::list\_ghostbuster\_requests\_elt, 229
  - attributes, 230
  - element\_name, 230
  - text\_attribute, 230
  - vcard, 230
- rpki::left\_right::list\_published\_objects\_elt, 231
  - attributes, 232
  - element\_name, 232
  - make\_reply, 231
  - obj, 232
  - serve\_dispatch, 232
  - text\_attribute, 232
- rpki::left\_right::list\_received\_resources\_elt, 233
  - attributes, 234
  - element\_name, 234
  - make\_reply, 233
  - serve\_dispatch, 233
- rpki::left\_right::list\_resources\_elt, 234
  - asn, 236

- attributes, 236
- element\_name, 236
- ipv4, 236
- ipv6, 236
- startElement, 235
- toXML, 235
- valid\_until, 237
- rpki::left\_right::list\_roa\_requests\_elt, 237
  - attributes, 238
  - element\_name, 238
  - ipv4, 238
  - ipv6, 238
  - startElement, 238
- rpki::left\_right::msg, 239
  - pdu, 239
  - serve\_top\_level, 239
  - version, 240
- rpki::left\_right::parent\_elt, 240
  - attributes, 243
  - booleans, 243
  - bpki\_cms\_cert, 243
  - bpki\_cms\_glue, 243
  - cas, 241
  - element\_name, 244
  - elements, 244
  - handles, 244
  - query\_up\_down, 241
  - repository, 241
  - serve\_post\_save\_hook, 242
  - serve\_reissue, 242
  - serve\_rekey, 242
  - serve\_revoke, 242
  - serve\_revoke\_forgotten, 242
  - sql\_template, 244
- rpki::left\_right::report\_error\_elt, 245
  - attributes, 246
  - element\_name, 246
  - error\_code, 246
  - error\_text, 246
  - from\_exception, 245
  - self\_handle, 246
  - tag, 246
  - text\_attribute, 247
- rpki::left\_right::repository\_elt, 247
  - attributes, 249
  - bpki\_cert, 249
  - bpki\_glue, 249
  - call\_pubd, 248
  - default\_pubd\_handler, 248
  - element\_name, 249
  - elements, 249
  - handles, 249
  - parents, 248
  - sql\_template, 250
- rpki::left\_right::sax\_handler, 250
  - name, 251
  - pdu, 251
  - version, 251
- rpki::left\_right::self\_elt, 251
  - attributes, 257
  - booleans, 257
  - bpki\_cert, 258
  - bpki\_glue, 258
  - bscs, 253
  - children, 253
  - client\_poll, 253
  - crl\_interval, 258
  - cron, 253
  - element\_name, 258
  - elements, 258
  - ghostbusters, 253
  - handles, 258
  - parents, 253
  - regen\_margin, 259
  - regenerate\_crls\_and\_manifests, 254
  - repositories, 254
  - roas, 254
  - serve\_fetch\_all, 254
  - serve\_fetch\_handle, 255
  - serve\_fetch\_one\_maybe, 255
  - serve\_post\_save\_hook, 255
  - serve\_publish\_world\_now, 255
  - serve\_reissue, 256
  - serve\_rekey, 256
  - serve\_revoke, 256
  - serve\_revoke\_forgotten, 256
  - serve\_run\_now, 256
  - sql\_template, 259
  - update\_children, 257
  - update\_ghostbusters, 257
  - update\_roas, 257
  - use\_hsm, 259

- rpki::log
  - debug, 85
  - enable\_trace, 85
  - error, 85
  - info, 85
  - init, 84
  - log\_repr, 84
  - note, 85
  - pid, 85
  - set\_trace, 84
  - show\_python\_ids, 85
  - tag, 86
  - trace, 84
  - traceback, 84
  - use\_syslog, 86
  - warn, 86
- rpki::log::logger, 259
  - \_\_call\_\_, 260
  - \_\_init\_\_, 260
  - priority, 260
- rpki::manifest::FileAndHash, 260
  - \_\_init\_\_, 261
  - file, 261
  - hash, 261
- rpki::manifest::FilesAndHashes, 261
  - \_\_init\_\_, 262
- rpki::manifest::Manifest, 262
  - \_\_init\_\_, 263
  - explicitVersion, 263
  - fileHashAlg, 263
  - fileList, 263
  - manifestNumber, 263
  - nextUpdate, 263
  - thisUpdate, 263
  - version, 264
- rpki::myrpki
  - allow\_incomplete, 90
  - b64\_equal, 89
  - etree\_post\_read, 89
  - etree\_pre\_write, 89
  - etree\_read, 89
  - etree\_validate, 89
  - etree\_write, 89
  - namespace, 90
  - namespaceQName, 90
  - PEMBase64, 90
  - PEMElement, 90
  - version, 91
  - whine, 91
- rpki::myrpki::CA, 264
  - \_\_init\_\_, 265
  - bsc, 265
  - cer, 268
  - cfg, 268
  - cms\_xml\_sign, 265
  - cms\_xml\_verify, 265
  - crl, 268
  - crlnum, 268
  - dir, 268
  - ee, 266
  - env, 269
  - fxcert, 266
  - index, 269
  - key, 269
  - openssl, 269
  - path\_restriction, 269
  - req, 269
  - run\_ca, 266
  - run\_dgst, 266
  - run\_openssl, 266
  - run\_req, 267
  - serial, 269
  - setup, 267
  - touch\_file, 267
  - xcert, 267
  - xcert\_filename, 267
  - xcert\_revoke, 268
- rpki::myrpki::child, 270
  - \_\_init\_\_, 271
  - \_\_repr\_\_, 271
  - add, 271
  - asns, 271
  - bpki\_certificate, 271
  - handle, 272
  - v4, 272
  - v4re, 272
  - v6, 272
  - v6re, 272
  - validity, 272
  - xml, 271
- rpki::myrpki::children, 273
  - add, 273

- from\_entitydb, 273
- xml, 273
- rpki::myrpki::comma\_set, 274
  - \_\_str\_\_, 274
- rpki::myrpki::csv\_reader, 274
  - \_\_init\_\_, 275
  - \_\_iter\_\_, 275
  - columns, 276
  - comment\_characters, 276
  - file, 276
  - filename, 276
  - min\_columns, 276
- rpki::myrpki::csv\_writer, 276
  - \_\_getattr\_\_, 277
  - \_\_init\_\_, 277
  - close, 277
  - file, 278
  - filename, 278
  - renmwo, 278
  - writer, 278
- rpki::myrpki::EntityDB, 278
  - \_\_call\_\_, 279
  - \_\_init\_\_, 279
  - dir, 279
  - identity, 279
  - iterate, 279
- rpki::myrpki::IRDB, 280
  - \_\_init\_\_, 280
  - close, 281
  - db, 281
  - update, 281
- rpki::myrpki::main, 282
  - \_\_init\_\_, 283
  - bpki\_resources, 289
  - bpki\_servers, 289
  - cfg, 289
  - cfg\_file, 289
  - complete\_delete\_child, 283
  - complete\_delete\_parent, 283
  - complete\_delete\_publication\_client, 283
  - complete\_delete\_repository, 284
  - complete\_renew\_child, 284
  - completedefault, 289
  - configure\_resources\_main, 284
  - default\_repository, 289
  - do\_configure\_child, 284
  - do\_configure\_daemons, 284
  - do\_configure\_parent, 285
  - do\_configure\_publication\_client, 285
  - do\_configure\_repository, 286
  - do\_configure\_resources, 286
  - do\_delete\_child, 286
  - do\_delete\_parent, 286
  - do\_delete\_publication\_client, 286
  - do\_delete\_repository, 287
  - do\_initialize, 287
  - do\_renew\_all\_children, 287
  - do\_renew\_child, 287
  - do\_update\_bpki, 287
  - entitydb, 289
  - entitydb\_complete, 288
  - handle, 289
  - help\_overview, 288
  - histfile, 290
  - prompt, 290
  - pubd\_contact\_info, 290
  - read\_config, 288
  - renew\_children\_common, 288
  - rsync\_module, 290
  - rsync\_server, 290
  - run\_pubd, 290
  - run\_rootd, 290
  - run\_rpkid, 291
  - show\_xml, 291
- rpki::myrpki::parent, 291
  - \_\_init\_\_, 292
  - \_\_repr\_\_, 292
  - add, 292
  - bpki\_cms\_certificate, 292
  - handle, 292
  - myhandle, 293
  - service\_uri, 293
  - sia\_base, 293
  - xml, 292
- rpki::myrpki::parents, 293
  - add, 294
  - from\_entitydb, 294
  - xml, 294
- rpki::myrpki::repositories, 294
  - add, 295
  - from\_entitydb, 295
  - xml, 295

- rpki::myrpki::repository, 295
  - \_\_init\_\_, 296
  - \_\_repr\_\_, 296
  - add, 296
  - bpki\_certificate, 297
  - handle, 297
  - service\_uri, 297
  - xml, 296
- rpki::myrpki::roa\_request, 297
  - \_\_init\_\_, 298
  - \_\_repr\_\_, 298
  - add, 298
  - asn, 299
  - group, 299
  - v4, 299
  - v4re, 299
  - v6, 299
  - v6re, 299
  - xml, 298
- rpki::myrpki::roa\_requests, 300
  - add, 300
  - from\_csv, 300
  - xml, 300
- rpki::oids
  - name2oid, 92
  - oid2name, 92
- rpki::pubd::main, 301
  - \_\_init\_\_, 302
  - bpki\_ta, 303
  - cfg, 303
  - cfg\_file, 303
  - client\_handler, 302
  - client\_url\_regexp, 303
  - control\_handler, 302
  - handler\_common, 302
  - http\_server\_host, 303
  - http\_server\_port, 303
  - irbe\_cert, 303
  - main, 302
  - profile, 303
  - pubd\_cert, 304
  - pubd\_key, 304
  - publication\_base, 304
  - publication\_multimodule, 304
  - sql, 304
- rpki::publication::certificate\_elt, 304
  - element\_name, 305
  - payload\_type, 305
- rpki::publication::client\_elt, 305
  - attributes, 307
  - base\_uri, 307
  - bpki\_cert, 307
  - bpki\_glue, 307
  - check\_allowed\_uri, 306
  - element\_name, 307
  - elements, 307
  - serve\_fetch\_all, 306
  - serve\_fetch\_one\_maybe, 306
  - sql\_template, 308
- rpki::publication::cms\_msg, 308
  - encoding, 308
  - saxify, 308
  - schema, 309
- rpki::publication::config\_elt, 309
  - attributes, 311
  - config\_id, 311
  - element\_name, 311
  - elements, 311
  - fetch, 310
  - serve\_fetch\_one\_maybe, 310
  - serve\_set, 310
  - sql\_template, 311
  - startElement, 310
  - wired\_in\_config\_id, 312
- rpki::publication::control\_elt, 312
  - serve\_dispatch, 312
- rpki::publication::crl\_elt, 313
  - element\_name, 313
  - payload\_type, 313
- rpki::publication::ghostbuster\_elt, 314
  - element\_name, 314
  - payload\_type, 314
- rpki::publication::manifest\_elt, 314
  - element\_name, 315
  - payload\_type, 315
- rpki::publication::msg, 315
  - pdus, 316
  - serve\_top\_level, 316
  - version, 316
- rpki::publication::publication\_namespace, 317
  - nsmap, 317

- xmlns, 317
- rpki::publication::publication\_object\_elt, 318
  - attributes, 320
  - endElement, 318
  - make\_publish, 319
  - make\_withdraw, 319
  - payload, 320
  - payload\_type, 321
  - raise\_if\_error, 319
  - serve\_dispatch, 319
  - serve\_publish, 319
  - serve\_withdraw, 320
  - toXML, 320
  - uri\_to\_filename, 320
- rpki::publication::report\_error\_elt, 321
  - \_\_str\_\_, 322
  - attributes, 322
  - element\_name, 323
  - error\_code, 323
  - error\_text, 323
  - from\_exception, 322
  - raise\_if\_error, 322
  - tag, 323
  - text\_attribute, 323
- rpki::publication::roa\_elt, 324
  - element\_name, 324
  - payload\_type, 324
- rpki::publication::sax\_handler, 324
  - name, 325
  - pdu, 325
  - version, 325
- rpki::relaxng
  - left\_right, 95
  - publication, 95
  - up\_down, 95
- rpki::resource\_set
  - \_bs2long, 97
  - \_long2bs, 97
  - \_rsplit, 97
  - inherit\_token, 98
  - re\_address\_range, 98
  - re\_asn\_range, 98
  - re\_prefix, 99
  - re\_prefix\_with\_maxlen, 99
  - test1, 97
  - test2, 98
  - test3, 98
  - testprefix, 98
- rpki::resource\_set::resource\_bag, 325
  - \_\_eq\_\_, 327
  - \_\_init\_\_, 326
  - \_\_ne\_\_, 327
  - \_\_str\_\_, 327
  - asn, 328
  - empty, 327
  - from\_inheritance, 327
  - from\_rfc3779\_tuples, 327
  - intersection, 327
  - oversized, 328
  - undersized, 328
  - union, 328
  - v4, 328
  - v6, 329
  - valid\_until, 329
- rpki::resource\_set::resource\_range, 329
  - \_\_cmp\_\_, 330
  - \_\_init\_\_, 330
  - max, 330
  - min, 330
- rpki::resource\_set::resource\_range\_as, 331
  - \_\_str\_\_, 331
  - datum\_type, 332
  - from\_strings, 331
  - min, 332
  - parse\_str, 332
  - to\_rfc3779\_tuple, 332
- rpki::resource\_set::resource\_range\_ip, 333
  - \_\_str\_\_, 333
  - \_prefixlen, 335
  - chop\_into\_prefixes, 333
  - from\_strings, 334
  - make\_prefix, 334
  - parse\_str, 334
  - prefixlen, 334
  - to\_rfc3779\_tuple, 334
- rpki::resource\_set::resource\_range\_ipv4, 335
  - datum\_type, 336
- rpki::resource\_set::resource\_range\_ipv6, 336
  - datum\_type, 336
- rpki::resource\_set::resource\_set, 337
  - \_\_init\_\_, 338
  - \_\_str\_\_, 338



- [\\_comm](#), 338
  - [append](#), 338
  - [canonical](#), 341
  - [canonize](#), 338
  - [contains](#), 339
  - [difference](#), 339
  - [extend](#), 339
  - [from\\_sql](#), 339
  - [inherit](#), 341
  - [intersection](#), 339
  - [issubset](#), 340
  - [issuperset](#), 340
  - [parse\\_str](#), 340
  - [symmetric\\_difference](#), 340
  - [union](#), 340
- [rpki::resource\\_set::resource\\_set\\_as](#), 341
  - [inherit](#), 342
  - [parse\\_rfc3779\\_tuple](#), 342
  - [range\\_type](#), 343
  - [to\\_rfc3779\\_tuple](#), 342
- [rpki::resource\\_set::resource\\_set\\_ip](#), 343
  - [inherit](#), 344
  - [parse\\_rfc3779\\_tuple](#), 344
  - [to\\_rfc3779\\_tuple](#), 344
  - [to\\_roa\\_prefix\\_set](#), 344
- [rpki::resource\\_set::resource\\_set\\_ipv4](#), 345
  - [afi](#), 345
  - [range\\_type](#), 345
- [rpki::resource\\_set::resource\\_set\\_ipv6](#), 346
  - [afi](#), 346
  - [range\\_type](#), 346
- [rpki::resource\\_set::roa\\_prefix](#), 347
  - [\\_\\_cmp\\_\\_](#), 348
  - [\\_\\_init\\_\\_](#), 348
  - [\\_\\_str\\_\\_](#), 348
  - [from\\_roa\\_tuple](#), 348
  - [max](#), 348
  - [max\\_prefixlen](#), 349
  - [min](#), 348
  - [parse\\_str](#), 349
  - [prefix](#), 349
  - [prefixlen](#), 350
  - [to\\_resource\\_range](#), 349
  - [to\\_roa\\_tuple](#), 349
- [rpki::resource\\_set::roa\\_prefix\\_ipv4](#), 350
  - [range\\_type](#), 350
- [rpki::resource\\_set::roa\\_prefix\\_ipv6](#), 351
  - [range\\_type](#), 351
- [rpki::resource\\_set::roa\\_prefix\\_set](#), 351
  - [\\_\\_init\\_\\_](#), 352
  - [\\_\\_str\\_\\_](#), 352
  - [from\\_sql](#), 352
  - [parse\\_str](#), 353
  - [to\\_resource\\_set](#), 353
  - [to\\_roa\\_tuple](#), 353
- [rpki::resource\\_set::roa\\_prefix\\_set\\_ipv4](#), 353
  - [prefix\\_type](#), 354
  - [resource\\_set\\_type](#), 354
- [rpki::resource\\_set::roa\\_prefix\\_set\\_ipv6](#), 354
  - [prefix\\_type](#), 355
  - [resource\\_set\\_type](#), 355
- [rpki::roa::ROAIPAddress](#), 355
  - [\\_\\_init\\_\\_](#), 356
  - [address](#), 356
  - [maxLength](#), 356
- [rpki::roa::ROAIPAddresses](#), 356
  - [\\_\\_init\\_\\_](#), 357
- [rpki::roa::ROAIPAddressFamilies](#), 357
  - [\\_\\_init\\_\\_](#), 357
- [rpki::roa::ROAIPAddressFamily](#), 358
  - [\\_\\_init\\_\\_](#), 358
  - [addresses](#), 358
  - [addressFamily](#), 358
- [rpki::roa::RouteOriginAttestation](#), 359
  - [\\_\\_init\\_\\_](#), 359
  - [asID](#), 360
  - [explicitVersion](#), 360
  - [ipAddrBlocks](#), 360
  - [version](#), 360
- [rpki::rootd](#)
  - [rootd](#), 101
- [rpki::rootd::cms\\_msg](#), 360
  - [saxify](#), 361
- [rpki::rootd::issue\\_pdu](#), 361
  - [serve\\_pdu](#), 361
- [rpki::rootd::list\\_pdu](#), 362
  - [serve\\_pdu](#), 362
- [rpki::rootd::main](#), 362
  - [\\_\\_init\\_\\_](#), 364
  - [bpki\\_ta](#), 365
  - [cfg](#), 365
  - [cfg\\_file](#), 365

- child\_bpki\_cert, 366
- compose\_response, 364
- del\_subject\_cert, 364
- del\_subject\_pkcs10, 364
- get\_root\_cert, 364
- get\_subject\_cert, 364
- get\_subject\_pkcs10, 364
- http\_server\_host, 366
- http\_server\_port, 366
- issue\_subject\_cert\_maybe, 365
- root\_newer\_than\_subject, 365
- rootd\_bpki\_cert, 366
- rootd\_bpki\_crl, 366
- rootd\_bpki\_key, 366
- rpki\_base\_uri, 366
- rpki\_class\_name, 367
- rpki\_root\_cert, 367
- rpki\_root\_cert\_file, 367
- rpki\_root\_cert\_uri, 367
- rpki\_root\_crl, 367
- rpki\_root\_dir, 367
- rpki\_root\_key, 367
- rpki\_root\_manifest, 368
- rpki\_subject\_cert, 368
- rpki\_subject\_lifetime, 368
- rpki\_subject\_pkcs10, 368
- rpki\_subject\_regen, 368
- set\_subject\_cert, 365
- set\_subject\_pkcs10, 365
- up\_down\_handler, 365
- rpki::rootd::message\_pdu, 368
  - log\_query, 369
  - name2type, 369
  - type2name, 369
- rpki::rootd::revoke\_pdu, 370
  - serve\_pdu, 370
- rpki::rootd::sax\_handler, 371
  - pdu, 371
- rpki::rpkid::ca\_detail\_obj, 371
  - activate, 373
  - ca, 373
  - ca\_cert\_uri, 378
  - ca\_id, 378
  - child\_certs, 373
  - create, 373
  - crl\_published, 378
  - crl\_published\_callback, 373
  - crl\_uri, 373
  - crl\_uri\_tail, 374
  - delete, 374
  - fetch\_child\_certs, 374
  - gctx, 378
  - generate\_crl, 374
  - generate\_manifest, 374
  - generate\_manifest\_cert, 375
  - ghostbusters, 375
  - has\_expired, 375
  - issue, 375
  - issue\_ee, 375
  - latest\_ca\_cert, 378
  - latest\_crl, 378
  - latest\_manifest, 378
  - latest\_manifest\_cert, 379
  - manifest\_private\_key\_id, 379
  - manifest\_public\_key, 379
  - manifest\_published, 379
  - manifest\_published\_callback, 376
  - manifest\_uri, 376
  - private\_key\_id, 379
  - public\_key, 379
  - reissue, 376
  - revoke, 376
  - revoked\_certs, 377
  - roas, 377
  - sql\_decode, 377
  - sql\_template, 379
  - state, 380
  - update, 377
- rpki::rpkid::ca\_obj, 380
  - active\_ca\_detail, 381
  - ca\_details, 381
  - check\_for\_updates, 381
  - construct\_sia\_uri, 382
  - create, 382
  - delete, 382
  - deprecated\_ca\_details, 382
  - gctx, 385
  - issue\_response\_candidate\_ca\_details, 383
  - last\_crl\_sn, 385
  - last\_issued\_sn, 385
  - last\_manifest\_sn, 385

- next\_crl\_number, 383
- next\_manifest\_number, 383
- next\_serial\_number, 383
- parent, 383
- parent\_id, 385
- parent\_resource\_class, 385
- pending\_ca\_details, 384
- reissue, 384
- rekey, 384
- revoke, 384
- revoked\_ca\_details, 384
- sia\_uri, 386
- sql\_template, 386
- rpki::rpkid::child\_cert\_obj, 386
  - \_\_init\_\_, 387
  - ca\_detail, 387
  - ca\_detail\_id, 389
  - cert, 389
  - child, 387
  - child\_id, 389
  - fetch, 388
  - gctx, 389
  - published, 390
  - published\_callback, 388
  - reissue, 388
  - revoke, 388
  - sql\_template, 390
  - uri, 389
  - uri\_tail, 389
- rpki::rpkid::ghostbuster\_obj, 390
  - \_\_init\_\_, 391
  - ca\_detail, 391
  - ca\_detail\_id, 394
  - cert, 394
  - gctx, 394
  - generate, 391
  - ghostbuster, 394
  - published, 394
  - published\_callback, 392
  - regenerate, 392
  - revoke, 392
  - self, 393
  - self\_id, 394
  - sql\_template, 394
  - update, 393
  - uri, 393
  - uri\_from\_key, 393
  - uri\_tail, 393
  - vcard, 395
- rpki::rpkid::main, 395
  - \_\_init\_\_, 396
  - bpki\_ta, 399
  - cfg, 399
  - cfg\_file, 399
  - checkpoint, 397
  - cron, 397
  - cron\_keepalive, 399
  - cron\_period, 399
  - cron\_timeout, 399
  - cron\_timer, 399
  - cronjob\_handler, 397
  - http\_server\_host, 400
  - http\_server\_port, 400
  - initial\_delay, 400
  - irbe\_cert, 400
  - irdb\_cert, 400
  - irdb\_query, 397
  - irdb\_query\_child\_resources, 397
  - irdb\_query\_ghostbuster\_requests, 398
  - irdb\_query\_roa\_requests, 398
  - irdb\_url, 400
  - left\_right\_handler, 398
  - main, 396
  - profile, 400
  - publication\_kludge\_base, 401
  - rpkid\_cert, 401
  - rpkid\_key, 401
  - sql, 401
  - start\_cron, 398
  - up\_down\_handler, 398
  - up\_down\_url\_regexp, 401
  - use\_internal\_cron, 401
- rpki::rpkid::publication\_queue, 402
  - \_\_init\_\_, 403
  - \_add, 403
  - call\_pubd, 403
  - handlers, 403
  - msgs, 403
  - publish, 403
  - replace, 404
  - repositories, 404
  - uris, 404

- withdraw, 403
- rpki::rpkid::revoked\_cert\_obj, 404
  - \_\_init\_\_, 405
  - ca\_detail, 405
  - ca\_detail\_id, 406
  - expires, 406
  - gctx, 406
  - revoke, 405
  - revoked, 406
  - serial, 406
  - sql\_template, 406
- rpki::rpkid::roa\_obj, 407
  - \_\_init\_\_, 408
  - \_\_repr\_\_, 408
  - asn, 411
  - ca\_detail, 408
  - ca\_detail\_id, 411
  - cert, 411
  - gctx, 412
  - generate, 408
  - ipv4, 412
  - ipv6, 412
  - published, 412
  - published\_callback, 409
  - regenerate, 409
  - revoke, 409
  - roa, 412
  - self, 410
  - self\_id, 412
  - sql\_delete\_hook, 410
  - sql\_fetch\_hook, 410
  - sql\_insert\_hook, 410
  - sql\_template, 412
  - update, 410
  - uri, 411
  - uri\_from\_key, 411
  - uri\_tail, 411
- rpki::sql::session, 413
  - \_\_init\_\_, 414
  - \_exceptions\_enabled, 416
  - \_wrap\_execute, 414
  - assert\_pristine, 414
  - cache, 416
  - cache\_clear, 414
  - close, 415
  - connect, 415
  - cur, 416
  - database, 416
  - db, 416
  - dirty, 417
  - execute, 415
  - executemany, 415
  - fetchall, 415
  - lastrowid, 415
  - password, 417
  - ping, 415
  - sweep, 416
  - username, 417
- rpki::sql::sql\_persistent, 417
  - gctx, 422
  - sql\_debug, 422
  - sql\_decode, 418
  - sql\_delete, 418
  - sql\_delete\_hook, 419
  - sql\_deleted, 422
  - sql\_encode, 419
  - sql\_fetch, 419
  - sql\_fetch\_all, 419
  - sql\_fetch\_hook, 420
  - sql\_fetch\_where, 420
  - sql\_fetch\_where1, 420
  - sql\_in\_db, 422
  - sql\_init, 420
  - sql\_insert\_hook, 420
  - sql\_is\_dirty, 421
  - sql\_mark\_clean, 421
  - sql\_mark\_deleted, 421
  - sql\_mark\_dirty, 421
  - sql\_store, 421
  - sql\_update\_hook, 422
- rpki::sql::template, 423
  - \_\_init\_\_, 423
  - columns, 424
  - delete, 424
  - index, 424
  - insert, 424
  - map, 424
  - select, 424
  - table, 424
  - update, 424
- rpki::sundial
  - \_cast, 104

- now, [104](#)
- test, [105](#)
- rpki::sundial::datetime, [425](#)
  - \_\_add\_\_, [426](#)
  - \_\_radd\_\_, [426](#)
  - \_\_rsub\_\_, [426](#)
  - \_\_str\_\_, [426](#)
  - \_\_sub\_\_, [426](#)
  - earlier, [426](#)
  - from\_sql, [427](#)
  - fromASN1tuple, [427](#)
  - fromdatetime, [427](#)
  - fromGeneralizedTime, [427](#)
  - fromOpenSSL, [427](#)
  - fromUTCTime, [427](#)
  - fromXMLtime, [428](#)
  - later, [428](#)
  - PKIX\_threshold, [429](#)
  - to\_sql, [428](#)
  - toASN1tuple, [428](#)
  - toGeneralizedTime, [428](#)
  - totimestamp, [429](#)
  - toUTCTime, [429](#)
  - toXMLtime, [429](#)
- rpki::sundial::timedelta, [430](#)
  - \_\_abs\_\_, [431](#)
  - \_\_add\_\_, [431](#)
  - \_\_div\_\_, [431](#)
  - \_\_floordiv\_\_, [431](#)
  - \_\_mul\_\_, [431](#)
  - \_\_neg\_\_, [431](#)
  - \_\_pos\_\_, [432](#)
  - \_\_radd\_\_, [432](#)
  - \_\_rdiv\_\_, [432](#)
  - \_\_rfloordiv\_\_, [432](#)
  - \_\_rmul\_\_, [432](#)
  - \_\_rsub\_\_, [432](#)
  - \_\_sub\_\_, [432](#)
  - convert\_to\_seconds, [433](#)
  - fromtimedelta, [433](#)
  - parse, [433](#)
  - regexp, [433](#)
  - years\_to\_seconds, [434](#)
- rpki::up\_down
  - nsmap, [106](#)
  - xmlns, [106](#)
- rpki::up\_down::base\_elt, [434](#)
  - check\_response, [434](#)
  - endElement, [435](#)
  - make\_b64elt, [435](#)
  - make\_elt, [435](#)
  - serve\_pdu, [435](#)
  - startElement, [435](#)
- rpki::up\_down::certificate\_elt, [436](#)
  - cert, [437](#)
  - cert\_url, [437](#)
  - endElement, [437](#)
  - req\_resource\_set\_as, [437](#)
  - req\_resource\_set\_ipv4, [438](#)
  - req\_resource\_set\_ipv6, [438](#)
  - startElement, [437](#)
  - toXML, [437](#)
- rpki::up\_down::class\_elt, [438](#)
  - \_\_init\_\_, [439](#)
  - cert\_url, [440](#)
  - certs, [440](#)
  - class\_name, [440](#)
  - endElement, [439](#)
  - from\_resource\_bag, [439](#)
  - issuer, [440](#)
  - resource\_set\_as, [441](#)
  - resource\_set\_ipv4, [441](#)
  - resource\_set\_ipv6, [441](#)
  - resource\_set\_notafter, [441](#)
  - startElement, [439](#)
  - suggested\_sia\_head, [441](#)
  - to\_resource\_bag, [440](#)
  - toXML, [440](#)
- rpki::up\_down::class\_response\_syntax, [441](#)
  - \_\_init\_\_, [442](#)
  - classes, [443](#)
  - startElement, [442](#)
  - toXML, [442](#)
- rpki::up\_down::cms\_msg, [443](#)
  - encoding, [443](#)
  - saxify, [443](#)
  - schema, [443](#)
- rpki::up\_down::error\_response\_pdu, [444](#)
  - \_\_init\_\_, [445](#)
  - check\_response, [445](#)
  - codes, [446](#)
  - description, [446](#)

- endElement, 445
- exceptions, 446
- status, 446
- toXML, 445
- rpki::up\_down::issue\_pdu, 447
  - class\_name, 448
  - endElement, 447
  - pkcs10, 448
  - query, 447
  - req\_resource\_set\_as, 449
  - req\_resource\_set\_ipv4, 449
  - req\_resource\_set\_ipv6, 449
  - serve\_pdu, 448
  - startElement, 448
  - toXML, 448
- rpki::up\_down::issue\_response\_pdu, 449
  - check\_response, 450
- rpki::up\_down::list\_pdu, 450
  - query, 450
  - serve\_pdu, 450
  - toXML, 451
- rpki::up\_down::list\_response\_pdu, 451
- rpki::up\_down::message\_pdu, 451
  - \_\_str\_\_, 452
  - log\_query, 452
  - make\_query, 453
  - name2type, 454
  - payload, 454
  - recipient, 454
  - sender, 454
  - serve\_error, 453
  - serve\_top\_level, 453
  - startElement, 453
  - toXML, 454
  - type, 454
  - type2name, 455
  - version, 455
- rpki::up\_down::multi\_uri, 455
  - \_\_init\_\_, 456
  - \_\_str\_\_, 456
  - rsync, 456
- rpki::up\_down::revoke\_pdu, 456
  - class\_name, 458
  - get\_SKI, 457
  - query, 457
  - serve\_pdu, 457
  - ski, 458
- rpki::up\_down::revoke\_response\_pdu, 458
- rpki::up\_down::revoke\_syntax, 458
  - class\_name, 460
  - ski, 460
  - startElement, 459
  - toXML, 459
- rpki::up\_down::sax\_handler, 460
  - name, 460
  - pdu, 461
  - version, 461
- rpki::x509
  - \_find\_xia\_uri, 108
  - base64\_with\_linebreaks, 108
  - calculate\_SKI, 108
  - POWify\_OID, 108
- rpki::x509::CMS\_object, 461
  - content, 464
  - debug\_cms\_certs, 464
  - DER, 464
  - dump\_on\_verify\_failure, 465
  - econtent\_oid, 465
  - extract, 462
  - formats, 465
  - get\_content, 463
  - get\_DER, 463
  - get\_POW, 463
  - get\_signingTime, 463
  - other\_clear, 465
  - pem\_converter, 465
  - POW, 466
  - print\_on\_der\_error, 466
  - require\_crls, 466
  - set\_content, 463
  - sign, 464
  - verify, 464
- rpki::x509::CRL, 466
  - DER, 469
  - formats, 469
  - generate, 467
  - get\_DER, 467
  - get\_POW, 468
  - get\_POWpkix, 468
  - getIssuer, 468
  - getNextUpdate, 468
  - getThisUpdate, 468

- pem\_converter, 469
- POW, 469
- POWpkix, 469
- rpki::x509::DeadDrop, 470
  - \_\_init\_\_, 470
  - dump, 471
  - maildir, 471
  - pid, 471
- rpki::x509::DER\_CMS\_object, 471
  - content, 472
  - decode, 472
  - encode, 472
- rpki::x509::DER\_object, 472
  - \_\_cmp\_\_, 474
  - \_\_init\_\_, 474
  - check, 474
  - check\_auto\_update, 474
  - clear, 474
  - DER, 479
  - dumpasn1, 475
  - empty, 475
  - filename, 479
  - formats, 479
  - from\_sql, 475
  - gAKI, 475
  - get\_3779resources, 475
  - get\_AIA, 476
  - get\_aia\_uri, 476
  - get\_AKI, 476
  - get\_Base64, 476
  - get\_basicConstraints, 476
  - get\_DER, 477
  - get\_PEM, 477
  - get\_SIA, 477
  - get\_sia\_directory\_uri, 477
  - get\_sia\_manifest\_uri, 477
  - get\_SKI, 478
  - gSKI, 478
  - hAKI, 478
  - hSKI, 478
  - is\_CA, 478
  - other\_clear, 480
  - pem\_converter, 480
  - set, 479
  - timestamp, 480
  - to\_sql, 479
- rpki::x509::Ghostbuster, 480
  - build, 481
  - content, 482
  - decode, 481
  - econtent\_oid, 482
  - encode, 481
  - pem\_converter, 482
- rpki::x509::PEM\_converter, 482
  - \_\_init\_\_, 483
  - b, 484
  - e, 484
  - looks\_like\_PEM, 483
  - to\_DER, 483
  - to\_PEM, 483
- rpki::x509::PKCS10, 484
  - check\_valid\_rpki, 485
  - create, 485
  - create\_ca, 485
  - DER, 486
  - formats, 486
  - get\_DER, 486
  - get\_POWpkix, 486
  - getPublicKey, 486
  - pem\_converter, 487
  - POWpkix, 487
- rpki::x509::ROA, 487
  - build, 488
  - content\_class, 488
  - econtent\_oid, 488
  - pem\_converter, 488
- rpki::x509::RSA, 489
  - DER, 491
  - formats, 491
  - generate, 490
  - get\_DER, 490
  - get\_POW, 490
  - get\_public\_DER, 490
  - get\_RSAPublic, 490
  - get\_SKI, 490
  - pem\_converter, 491
  - POW, 491
- rpki::x509::RSAPublic, 492
  - DER, 493
  - formats, 493
  - get\_DER, 492
  - get\_POW, 493

- get\_SKI, 493
- pem\_converter, 493
- POW, 494
- rpki::x509::SignedManifest, 494
  - build, 495
  - content\_class, 495
  - econtent\_oid, 495
  - getNextUpdate, 495
  - getThisUpdate, 495
  - pem\_converter, 495
- rpki::x509::X509, 496
  - cross\_certify, 497
  - DER, 500
  - expired, 497
  - formats, 500
  - get\_DER, 497
  - get\_POW, 498
  - get\_POWpkix, 498
  - getIssuer, 498
  - getNotAfter, 498
  - getNotBefore, 498
  - getPublicKey, 498
  - getSerial, 499
  - getSubject, 499
  - issue, 499
  - normalize\_chain, 499
  - pem\_converter, 500
  - POW, 500
  - POWpkix, 500
- rpki::x509::XML\_CMS\_object, 501
  - content, 503
  - decode, 501
  - dump\_inbound\_cms, 503
  - dump\_outbound\_cms, 503
  - dump\_to\_disk, 502
  - econtent\_oid, 503
  - encode, 502
  - pretty\_print\_content, 502
  - schema\_check, 502
  - unwrap, 502
  - wrap, 502
- rpki::xml\_utils::base\_elt, 504
  - \_\_str\_\_, 505
  - attributes, 506
  - booleans, 506
  - elements, 507
  - endElement, 505
  - make\_b64elt, 505
  - make\_elt, 505
  - make\_pdu, 505
  - read\_attrs, 505
  - startElement, 506
  - toXML, 506
- rpki::xml\_utils::data\_elt, 507
  - endElement, 508
  - make\_reply, 508
  - make\_reply\_clone\_hook, 508
  - serve\_create, 508
  - serve\_destroy, 509
  - serve\_destroy\_hook, 509
  - serve\_dispatch, 509
  - serve\_fetch\_one, 509
  - serve\_get, 509
  - serve\_list, 510
  - serve\_post\_save\_hook, 510
  - serve\_pre\_save\_hook, 510
  - serve\_set, 510
  - toXML, 510
  - unimplemented\_control, 511
- rpki::xml\_utils::msg, 511
  - \_\_str\_\_, 512
  - endElement, 512
  - is\_query, 512
  - is\_reply, 512
  - query, 512
  - reply, 513
  - startElement, 513
  - toXML, 513
  - type, 513
  - version, 513
- rpki::xml\_utils::sax\_handler, 514
  - \_\_init\_\_, 515
  - characters, 515
  - create\_top\_level, 515
  - endElement, 515
  - endElementNS, 515
  - result, 516
  - saxify, 515
  - stack, 516
  - startElement, 516
  - startElementNS, 516
  - text, 516



- rpki::xml\_utils::text\_elt, 517
  - endElement, 517
  - text\_attribute, 518
  - toXML, 517
- rpki\_base\_uri
  - rpki::rootd::main, 366
- rpki\_class\_name
  - rpki::rootd::main, 367
- rpki\_content\_type
  - rpki::http, 78
- rpki\_root\_cert
  - rpki::rootd::main, 367
- rpki\_root\_cert\_file
  - rpki::rootd::main, 367
- rpki\_root\_cert\_uri
  - rpki::rootd::main, 367
- rpki\_root\_crl
  - rpki::rootd::main, 367
- rpki\_root\_dir
  - rpki::rootd::main, 367
- rpki\_root\_key
  - rpki::rootd::main, 367
- rpki\_root\_manifest
  - rpki::rootd::main, 368
- rpki\_subject\_cert
  - rpki::rootd::main, 368
- rpki\_subject\_lifetime
  - rpki::rootd::main, 368
- rpki\_subject\_pkcs10
  - rpki::rootd::main, 368
- rpki\_subject\_regen
  - rpki::rootd::main, 368
- rpkid, 109
- rpkid.py(3569), 535
- rpkid.py(3793), 535
- rpkid\_cert
  - rpki::irdbd::main, 216
  - rpki::rpkid::main, 401
- rpkid\_key
  - rpki::rpkid::main, 401
- rsync
  - rpki::up\_down::multi\_uri, 456
- rsync\_module
  - rpki::myrpki::main, 290
- rsync\_server
  - rpki::myrpki::main, 290
- run\_ca
  - rpki::myrpki::CA, 266
- run\_debug
  - rpki::async::timer, 153
- run\_deferred
  - rpki::async, 67
- run\_dgst
  - rpki::myrpki::CA, 266
- run\_openssl
  - rpki::myrpki::CA, 266
- run\_pubd
  - rpki::myrpki::main, 290
- run\_req
  - rpki::myrpki::CA, 267
- run\_rootd
  - rpki::myrpki::main, 290
- run\_rpkid
  - rpki::myrpki::main, 291
- runq
  - rpki::async::timer, 151
- saxify
  - irbe\_cli::left\_right\_cms\_msg, 119
  - irbe\_cli::publication\_cms\_msg, 124
  - rpki::left\_right::cms\_msg, 225
  - rpki::publication::cms\_msg, 308
  - rpki::rootd::cms\_msg, 361
  - rpki::up\_down::cms\_msg, 443
  - rpki::xml\_utils::sax\_handler, 515
- schema
  - rpki::left\_right::cms\_msg, 225
  - rpki::publication::cms\_msg, 309
  - rpki::up\_down::cms\_msg, 443
- schema\_check
  - rpki::x509::XML\_CMS\_object, 502
- seconds\_until\_wakeup
  - rpki::async::timer, 152
- select
  - rpki::sql::template, 424
- self
  - rpki::left\_right::data\_elt, 227
  - rpki::rpkid::ghostbuster\_obj, 393
  - rpki::rpkid::roa\_obj, 410
- self\_handle
  - rpki::left\_right::data\_elt, 228
  - rpki::left\_right::report\_error\_elt, 246

- self\_id
  - rpki::left\_right::data\_elt, 228
  - rpki::rpkid::ghostbuster\_obj, 394
  - rpki::rpkid::roa\_obj, 412
- send\_error
  - rpki::http::http\_server, 204
- send\_message
  - rpki::http::http\_server, 204
- send\_reply
  - rpki::http::http\_server, 204
- send\_request
  - rpki::http::http\_client, 188
  - rpki::http::http\_queue, 197
- sender
  - rpki::up\_down::message\_pdu, 454
- Sequence, 518
- SequenceOf, 518
- serial
  - rpki::myrpki::CA, 269
  - rpki::rpkid::revoked\_cert\_obj, 406
- serve\_create
  - rpki::xml\_utils::data\_elt, 508
- serve\_destroy
  - rpki::xml\_utils::data\_elt, 509
- serve\_destroy\_hook
  - rpki::left\_right::child\_elt, 222
  - rpki::xml\_utils::data\_elt, 509
- serve\_dispatch
  - rpki::left\_right::list\_published\_objects\_ - elt, 232
  - rpki::left\_right::list\_received\_resources elt, 233
  - rpki::publication::control\_elt, 312
  - rpki::publication::publication\_object\_ - elt, 319
  - rpki::xml\_utils::data\_elt, 509
- serve\_error
  - rpki::up\_down::message\_pdu, 453
- serve\_fetch\_all
  - rpki::left\_right::data\_elt, 227
  - rpki::left\_right::self\_elt, 254
  - rpki::publication::client\_elt, 306
- serve\_fetch\_handle
  - rpki::left\_right::data\_elt, 227
  - rpki::left\_right::self\_elt, 255
- serve\_fetch\_one
  - rpki::xml\_utils::data\_elt, 509
- serve\_fetch\_one\_maybe
  - rpki::left\_right::data\_elt, 227
  - rpki::left\_right::self\_elt, 255
  - rpki::publication::client\_elt, 306
  - rpki::publication::config\_elt, 310
- serve\_get
  - rpki::xml\_utils::data\_elt, 509
- serve\_list
  - rpki::xml\_utils::data\_elt, 510
- serve\_pdu
  - rpki::rootd::issue\_pdu, 361
  - rpki::rootd::list\_pdu, 362
  - rpki::rootd::revoke\_pdu, 370
  - rpki::up\_down::base\_elt, 435
  - rpki::up\_down::issue\_pdu, 448
  - rpki::up\_down::list\_pdu, 450
  - rpki::up\_down::revoke\_pdu, 457
- serve\_post\_save\_hook
  - rpki::left\_right::child\_elt, 222
  - rpki::left\_right::parent\_elt, 242
  - rpki::left\_right::self\_elt, 255
  - rpki::xml\_utils::data\_elt, 510
- serve\_pre\_save\_hook
  - rpki::left\_right::bsc\_elt, 218
  - rpki::left\_right::data\_elt, 227
  - rpki::xml\_utils::data\_elt, 510
- serve\_publish
  - rpki::publication::publication\_object\_ - elt, 319
- serve\_publish\_world\_now
  - rpki::left\_right::self\_elt, 255
- serve\_reissue
  - rpki::left\_right::child\_elt, 222
  - rpki::left\_right::parent\_elt, 242
  - rpki::left\_right::self\_elt, 256
- serve\_rekey
  - rpki::left\_right::parent\_elt, 242
  - rpki::left\_right::self\_elt, 256
- serve\_revoke
  - rpki::left\_right::parent\_elt, 242
  - rpki::left\_right::self\_elt, 256
- serve\_revoke\_forgotten
  - rpki::left\_right::parent\_elt, 242
  - rpki::left\_right::self\_elt, 256
- serve\_run\_now

- rpki::left\_right::self\_elt, 256
- serve\_set
  - rpki::publication::config\_elt, 310
  - rpki::xml\_utils::data\_elt, 510
- serve\_top\_level
  - rpki::left\_right::msg, 239
  - rpki::publication::msg, 316
  - rpki::up\_down::message\_pdu, 453
- serve\_up\_down
  - rpki::left\_right::child\_elt, 223
- serve\_withdraw
  - rpki::publication::publication\_object\_elt, 320
- server
  - rpki::http, 76
- server\_cert
  - irbe\_cli, 61
  - rpki::http::caller, 185
- server\_ta
  - irbe\_cli, 61
  - rpki::http::caller, 185
- service\_uri
  - rpki::myrpki::parent, 293
  - rpki::myrpki::repository, 297
- set, 518
  - rpki::async::timer, 152
  - rpki::x509::DER\_object, 479
- set\_content
  - rpki::x509::CMS\_object, 463
- set\_errback
  - rpki::async::timer, 152
- set\_global\_flags
  - rpki::config::parser, 160
- set\_handler
  - rpki::async::timer, 152
- set\_state
  - rpki::http::http\_client, 188
- set\_subject\_cert
  - rpki::rootd::main, 365
- set\_subject\_pkcs10
  - rpki::rootd::main, 365
- set\_trace
  - rpki::log, 84
- setup
  - rpki::myrpki::CA, 267
- show\_python\_ids
  - rpki::log, 85
- show\_tracebacks
  - rpki::http::http\_listener, 192
  - rpki::http::http\_stream, 210
- show\_xml
  - rpki::myrpki::main, 291
- sia\_base
  - rpki::myrpki::parent, 293
- sia\_uri
  - rpki::rpkid::ca\_obj, 386
- sign
  - rpki::x509::CMS\_object, 464
- signing\_cert
  - irbe\_cli::bsc\_elt, 112
  - rpki::left\_right::bsc\_elt, 220
- signing\_cert\_crl
  - irbe\_cli::bsc\_elt, 112
  - rpki::left\_right::bsc\_elt, 220
- ski
  - rpki::up\_down::revoke\_pdu, 458
  - rpki::up\_down::revoke\_syntax, 460
- socket\_cb
  - rpki::adns::query, 137
- socket\_eb
  - rpki::adns::query, 137
- socket\_timeout
  - rpki::adns::query, 138
- sockets
  - rpki::adns::query, 139
- software\_name
  - rpki::http::http\_message, 195
- sql
  - rpki::pubd::main, 304
  - rpki::rpkid::main, 401
- sql.py(3551), 535
- sql\_debug
  - rpki::sql::sql\_persistent, 422
- sql\_decode
  - rpki::rpkid::ca\_detail\_obj, 377
  - rpki::sql::sql\_persistent, 418
- sql\_delete
  - rpki::sql::sql\_persistent, 418
- sql\_delete\_hook
  - rpki::rpkid::roa\_obj, 410
  - rpki::sql::sql\_persistent, 419
- sql\_deleted

- rpki::sql::sql\_persistent, 422
- sql\_encode
  - rpki::sql::sql\_persistent, 419
- sql\_fetch
  - rpki::sql::sql\_persistent, 419
- sql\_fetch\_all
  - rpki::sql::sql\_persistent, 419
- sql\_fetch\_hook
  - rpki::rpkid::roa\_obj, 410
  - rpki::sql::sql\_persistent, 420
- sql\_fetch\_where
  - rpki::sql::sql\_persistent, 420
- sql\_fetch\_where1
  - rpki::sql::sql\_persistent, 420
- sql\_in\_db
  - rpki::sql::sql\_persistent, 422
- sql\_init
  - rpki::sql::sql\_persistent, 420
- sql\_insert\_hook
  - rpki::rpkid::roa\_obj, 410
  - rpki::sql::sql\_persistent, 420
- sql\_is\_dirty
  - rpki::sql::sql\_persistent, 421
- sql\_mark\_clean
  - rpki::sql::sql\_persistent, 421
- sql\_mark\_deleted
  - rpki::sql::sql\_persistent, 421
- sql\_mark\_dirty
  - rpki::sql::sql\_persistent, 421
- sql\_store
  - rpki::sql::sql\_persistent, 421
- sql\_template
  - rpki::left\_right::bsc\_elt, 220
  - rpki::left\_right::child\_elt, 224
  - rpki::left\_right::parent\_elt, 244
  - rpki::left\_right::repository\_elt, 250
  - rpki::left\_right::self\_elt, 259
  - rpki::publication::client\_elt, 308
  - rpki::publication::config\_elt, 311
  - rpki::rpkid::ca\_detail\_obj, 379
  - rpki::rpkid::ca\_obj, 386
  - rpki::rpkid::child\_cert\_obj, 390
  - rpki::rpkid::ghostbuster\_obj, 394
  - rpki::rpkid::revoked\_cert\_obj, 406
  - rpki::rpkid::roa\_obj, 412
- sql\_update\_hook
  - rpki::sql::sql\_persistent, 422
- stack
  - rpki::xml\_utils::sax\_handler, 516
- start
  - rpki::adns::query, 139
  - rpki::http::http\_client, 189
- start\_cron
  - rpki::rpkid::main, 398
- startElement
  - rpki::left\_right::list\_resources\_elt, 235
  - rpki::left\_right::list\_roa\_requests\_elt, 238
  - rpki::publication::config\_elt, 310
  - rpki::up\_down::base\_elt, 435
  - rpki::up\_down::certificate\_elt, 437
  - rpki::up\_down::class\_elt, 439
  - rpki::up\_down::class\_response\_syntax, 442
  - rpki::up\_down::issue\_pdu, 448
  - rpki::up\_down::message\_pdu, 453
  - rpki::up\_down::revoke\_syntax, 459
  - rpki::xml\_utils::base\_elt, 506
  - rpki::xml\_utils::msg, 513
  - rpki::xml\_utils::sax\_handler, 516
- startElementNS
  - rpki::xml\_utils::sax\_handler, 516
- state
  - rpki::http::http\_client, 190
  - rpki::rpkid::ca\_detail\_obj, 380
- status
  - rpki::up\_down::error\_response\_pdu, 446
- suggested\_sia\_head
  - rpki::up\_down::class\_elt, 441
- sundial.py(3783), 536
- supported\_address\_families
  - rpki::http, 76
- sweep
  - rpki::sql::session, 416
- symmetric\_difference
  - rpki::resource\_set::resource\_set, 340
- table
  - rpki::sql::template, 424
- tag
  - rpki::left\_right::report\_error\_elt, 246
  - rpki::log, 86

---

rpki::publication::report\_error\_elt, 323  
 test  
   rpki::sundial, 105  
 test1  
   rpki::resource\_set, 97  
 test2  
   rpki::resource\_set, 98  
 test3  
   rpki::resource\_set, 98  
 testprefix  
   rpki::resource\_set, 98  
 text  
   rpki::xml\_utils::sax\_handler, 516  
 text\_attribute  
   rpki::left\_right::list\_ghostbuster\_requests\_elt, 230  
   rpki::left\_right::list\_published\_objects\_elt, 232  
   rpki::left\_right::report\_error\_elt, 247  
   rpki::publication::report\_error\_elt, 323  
   rpki::xml\_utils::text\_elt, 518  
 textwrap::TextWrapper, 519  
 thisUpdate  
   rpki::manifest::Manifest, 263  
 threshold  
   rpki::async::gc\_summary, 144  
 timeout  
   rpki::http::http\_client, 190  
   rpki::http::http\_server, 205  
 timer  
   rpki::adns::query, 139  
   rpki::async::gc\_summary, 144  
   rpki::http::http\_stream, 210  
 timestamp  
   rpki::x509::DER\_object, 480  
 to\_bytes  
   rpki::ipaddr::v4addr, 212  
   rpki::ipaddr::v6addr, 213  
 to\_DER  
   rpki::x509::PEM\_converter, 483  
 to\_PEM  
   rpki::x509::PEM\_converter, 483  
 to\_resource\_bag  
   rpki::up\_down::class\_elt, 440  
 to\_resource\_range  
   rpki::resource\_set::roa\_prefix, 349  
   rpki::resource\_set  
   rpki::resource\_set::roa\_prefix\_set, 353  
   to\_rfc3779\_tuple  
   rpki::resource\_set::resource\_range\_as, 332  
   rpki::resource\_set::resource\_range\_ip, 334  
   rpki::resource\_set::resource\_set\_as, 342  
   rpki::resource\_set::resource\_set\_ip, 344  
   to\_roa\_prefix\_set  
   rpki::resource\_set::resource\_set\_ip, 344  
   to\_roa\_tuple  
   rpki::resource\_set::roa\_prefix, 349  
   rpki::resource\_set::roa\_prefix\_set, 353  
   rpki::sundial::datetime, 428  
   rpki::x509::DER\_object, 479  
   toASN1tuple  
   rpki::sundial::datetime, 428  
   toGeneralizedTime  
   rpki::sundial::datetime, 428  
   top\_opts  
   irbe\_cli, 61  
   totimestamp  
   rpki::sundial::datetime, 429  
   touch\_file  
   rpki::myrpki::CA, 267  
   toUTCTime  
   rpki::sundial::datetime, 429  
   toXML  
   rpki::left\_right::list\_resources\_elt, 235  
   rpki::publication::publication\_object\_elt, 320  
   rpki::up\_down::certificate\_elt, 437  
   rpki::up\_down::class\_elt, 440  
   rpki::up\_down::class\_response\_syntax, 442  
   rpki::up\_down::error\_response\_pdu, 445  
   rpki::up\_down::issue\_pdu, 448  
   rpki::up\_down::list\_pdu, 451  
   rpki::up\_down::message\_pdu, 454  
   rpki::up\_down::revoke\_syntax, 459  
   rpki::xml\_utils::base\_elt, 506  
   rpki::xml\_utils::data\_elt, 510  
   rpki::xml\_utils::msg, 513  
   rpki::xml\_utils::text\_elt, 517

- toXMLtime
  - rpki::sundial::datetime, 429
- trace
  - rpki::async::timer, 153
  - rpki::log, 84
- traceback
  - rpki::log, 84
- type
  - rpki::up\_down::message\_pdu, 454
  - rpki::xml\_utils::msg, 513
- type2name
  - rpki::rootd::message\_pdu, 369
  - rpki::up\_down::message\_pdu, 455
- typemap
  - rpki::adns::getaddrinfo, 134
- undersized
  - rpki::resource\_set::resource\_bag, 328
- unimplemented\_control
  - rpki::xml\_utils::data\_elt, 511
- union
  - rpki::resource\_set::resource\_bag, 328
  - rpki::resource\_set::resource\_set, 340
- unwind\_stack
  - rpki::async::iterator, 146
- unwrap
  - rpki::x509::XML\_CMS\_object, 502
- up\_down
  - rpki::relaxng, 95
- up\_down.py(3746), 536
- up\_down\_handler
  - rpki::rootd::main, 365
  - rpki::rpkid::main, 398
- up\_down\_url\_regexp
  - rpki::rpkid::main, 401
- update
  - rpki::myrpki::IRDB, 281
  - rpki::rpkid::ca\_detail\_obj, 377
  - rpki::rpkid::ghostbuster\_obj, 393
  - rpki::rpkid::roa\_obj, 410
  - rpki::sql::template, 424
- update\_children
  - rpki::left\_right::self\_elt, 257
- update\_ghostbusters
  - rpki::left\_right::self\_elt, 257
- update\_roas
  - rpki::left\_right::self\_elt, 257
- update\_timeout
  - rpki::http::http\_stream, 209
- uri
  - rpki::rpkid::child\_cert\_obj, 389
  - rpki::rpkid::ghostbuster\_obj, 393
  - rpki::rpkid::roa\_obj, 411
- uri\_from\_key
  - rpki::rpkid::ghostbuster\_obj, 393
  - rpki::rpkid::roa\_obj, 411
- uri\_tail
  - rpki::rpkid::child\_cert\_obj, 389
  - rpki::rpkid::ghostbuster\_obj, 393
  - rpki::rpkid::roa\_obj, 411
- uri\_to\_filename
  - rpki::publication::publication\_object\_ - elt, 320
- uris
  - rpki::rpkid::publication\_queue, 404
- url
  - irbe\_cli, 61
  - rpki::http::caller, 185
- usage
  - irbe\_cli, 59
  - irbe\_cli::cmd\_elt\_mixin, 115
  - irbe\_cli::cmd\_msg\_mixin, 117
- usage\_fill
  - irbe\_cli, 61
- use\_adns
  - rpki::http, 78
- use\_hsm
  - rpki::left\_right::self\_elt, 259
- use\_internal\_cron
  - rpki::rpkid::main, 401
- use\_syslog
  - rpki::log, 86
- username
  - rpki::sql::session, 417
- v4
  - rpki::myrpki::child, 272
  - rpki::myrpki::roa\_request, 299
  - rpki::resource\_set::resource\_bag, 328
- v4re
  - rpki::myrpki::child, 272
  - rpki::myrpki::roa\_request, 299

- v6
  - rpki::myrpki::child, 272
  - rpki::myrpki::roa\_request, 299
  - rpki::resource\_set::resource\_bag, 329
- v6re
  - rpki::myrpki::child, 272
  - rpki::myrpki::roa\_request, 299
- valid\_until
  - rpki::left\_right::list\_resources\_elt, 237
  - rpki::resource\_set::resource\_bag, 329
- validity
  - rpki::myrpki::child, 272
- vcard
  - rpki::left\_right::list\_ghostbuster\_requests\_elt, 230
  - rpki::rpkid::ghostbuster\_obj, 395
- verbose
  - irbe\_cli, 61
- verify
  - rpki::x509::CMS\_object, 464
- version
  - rpki::http::http\_message, 195
  - rpki::left\_right::msg, 240
  - rpki::left\_right::sax\_handler, 251
  - rpki::manifest::Manifest, 264
  - rpki::myrpki, 91
  - rpki::publication::msg, 316
  - rpki::publication::sax\_handler, 325
  - rpki::roa::RouteOriginAttestation, 360
  - rpki::up\_down::message\_pdu, 455
  - rpki::up\_down::sax\_handler, 461
  - rpki::xml\_utils::msg, 513
- want\_persistent\_client
  - rpki::http, 78
- want\_persistent\_server
  - rpki::http, 78
- warn
  - rpki::log, 86
- when
  - rpki::async::timer, 153
- whine
  - rpki::myrpki, 91
- wired\_in\_config\_id
  - rpki::publication::config\_elt, 312
- withdraw
  - rpki::rpkid::publication\_queue, 403
- wrap
  - rpki::x509::XML\_CMS\_object, 502
- writable
  - rpki::adns::dispatcher, 131
- writer
  - rpki::myrpki::csv\_writer, 278
- x509.py(3793), 537
- xcert
  - rpki::myrpki::CA, 267
  - xcert\_filename
    - rpki::myrpki::CA, 267
  - xcert\_revoke
    - rpki::myrpki::CA, 268
- xml
  - rpki::myrpki::child, 271
  - rpki::myrpki::children, 273
  - rpki::myrpki::parent, 292
  - rpki::myrpki::parents, 294
  - rpki::myrpki::repositories, 295
  - rpki::myrpki::repository, 296
  - rpki::myrpki::roa\_request, 298
  - rpki::myrpki::roa\_requests, 300
  - xml::sax::handler::ContentHandler, 519
- xml\_utils.py(3725), 538
- xmlns
  - rpki::left\_right::left\_right\_namespace, 229
  - rpki::publication::publication\_namespace, 317
  - rpki::up\_down, 106
- years\_to\_seconds
  - rpki::sundial::timedelta, 434
- yes\_or\_no
  - rpki::cli, 68