

RPKI Engine

1.0

Generated by Doxygen 1.5.9

Fri Oct 23 00:02:29 2009

Contents

1	RPKI Engine Reference Manual	1
2	Further Reading	1
3	Installation Guide	2
4	Operation Guide	5
4.1	rpkid.py	6
4.2	pubd.py	7
4.3	rootd.py	8
4.4	irdbd.py	10
4.5	irbe_cli.py	11
4.6	cross_certify.py	13
4.7	irbe-setup.py config file	13
4.8	cronjob.py	14
4.9	testbed.py:	15
4.10	testpoke.py	17
5	Left-right protocol	18
5.1	Terminology	18
5.2	initiated by the IRBE	19
5.2.1	<self/> object	19
5.2.2	<bsc/> object	21
5.2.3	<parent/> object	22
5.2.4	<child/> object	23
5.2.5	<repository/> object	24
5.2.6	<route_origin/> object	25
5.3	Operations initiated by the RPKI engine	26
5.3.1	<list_resources/> messages	26
5.4	Error handling	27
6	Publication protocol	28

6.1	Terminology	28
6.2	Publication control subprotocol	28
6.2.1	<config/> object	29
6.2.2	<client/> object	29
6.3	Publication subprotocol	30
6.3.1	<certificate/> object	30
6.3.2	<crl/> object	30
6.3.3	<manifest/> object	30
6.3.4	<roa/> object	30
6.4	Error handling	30
6.5	Additional access control considerations.	31
7	SQL database schemas	32
7.1	rpkid SQL schema	34
7.2	pubd SQL Schema	38
7.3	irdbd SQL Schema	40
8	BPKI model	42
9	Namespace Documentation	45
9.1	Package irbe_cli	45
9.1.1	Detailed Description	46
9.1.2	Function Documentation	46
9.1.3	Variable Documentation	47
9.2	Package irdbd	49
9.2.1	Detailed Description	50
9.2.2	Function Documentation	50
9.2.3	Variable Documentation	51
9.3	Package pubd	53
9.3.1	Detailed Description	54
9.3.2	Function Documentation	54
9.3.3	Variable Documentation	55

9.4	Package rootd	55
9.4.1	Detailed Description	56
9.4.2	Function Documentation	57
9.4.3	Variable Documentation	59
9.5	Package rpki	63
9.6	Package rpki.async	63
9.6.1	Detailed Description	64
9.6.2	Function Documentation	64
9.6.3	Variable Documentation	65
9.7	Package rpki.config	65
9.7.1	Detailed Description	65
9.8	Package rpki.exceptions	66
9.8.1	Detailed Description	67
9.9	Package rpki.https	68
9.9.1	Detailed Description	68
9.9.2	Function Documentation	69
9.9.3	Variable Documentation	70
9.10	Package rpki.ipaddrs	71
9.10.1	Detailed Description	71
9.11	Package rpki.left_right	72
9.11.1	Detailed Description	73
9.11.2	Variable Documentation	73
9.12	Package rpki.log	74
9.12.1	Detailed Description	74
9.12.2	Function Documentation	75
9.12.3	Variable Documentation	76
9.13	Package rpki.manifest	77
9.13.1	Detailed Description	77
9.14	Package rpki.oids	78
9.14.1	Detailed Description	78
9.14.2	Variable Documentation	78

9.15	Package rpki.publication	79
9.15.1	Detailed Description	80
9.16	Package rpki.relaxng	80
9.16.1	Variable Documentation	81
9.17	Package rpki.resource_set	81
9.17.1	Detailed Description	82
9.17.2	Function Documentation	83
9.17.3	Variable Documentation	84
9.18	Package rpki.roa	84
9.18.1	Detailed Description	84
9.19	Package rpki.rpki_engine	85
9.19.1	Detailed Description	85
9.20	Package rpki.sql	86
9.20.1	Detailed Description	86
9.21	Package rpki.sundial	87
9.21.1	Detailed Description	87
9.21.2	Function Documentation	88
9.22	Package rpki.up_down	89
9.22.1	Detailed Description	89
9.22.2	Variable Documentation	90
9.23	Package rpki.x509	90
9.23.1	Detailed Description	91
9.23.2	Function Documentation	92
9.24	Package rpki.xml_utils	92
9.24.1	Detailed Description	92
9.25	Package rpkiid	93
9.25.1	Detailed Description	93
9.25.2	Function Documentation	94
9.25.3	Variable Documentation	94
10	Class Documentation	94

10.1	async_chat Class Reference	94
10.2	dispatcher Class Reference	95
10.3	Exception Class Reference	95
10.4	irbe_cli.bsc_elt Class Reference	95
10.4.1	Detailed Description	95
10.4.2	Member Function Documentation	96
10.4.3	Member Data Documentation	96
10.5	irbe_cli.caller Class Reference	97
10.5.1	Detailed Description	97
10.5.2	Member Function Documentation	97
10.5.3	Member Data Documentation	98
10.6	irbe_cli.certificate_elt Class Reference	99
10.6.1	Detailed Description	99
10.7	irbe_cli.child_elt Class Reference	99
10.7.1	Detailed Description	99
10.8	irbe_cli.client_elt Class Reference	99
10.8.1	Detailed Description	99
10.9	irbe_cli.cmd_elt_mixin Class Reference	99
10.9.1	Detailed Description	100
10.9.2	Member Function Documentation	101
10.9.3	Member Data Documentation	102
10.10	irbe_cli.cmd_msg_mixin Class Reference	103
10.10.1	Detailed Description	104
10.10.2	Member Function Documentation	104
10.11	irbe_cli.config_elt Class Reference	104
10.11.1	Detailed Description	104
10.11.2	Member Function Documentation	105
10.11.3	Member Data Documentation	105
10.12	irbe_cli.crl_elt Class Reference	105
10.12.1	Detailed Description	105
10.13	irbe_cli.left_right_cms_msg Class Reference	105

10.13.1 Detailed Description	106
10.13.2 Member Data Documentation	106
10.14irbe_cli.left_right_msg Class Reference	106
10.14.1 Detailed Description	106
10.14.2 Member Data Documentation	106
10.15irbe_cli.left_right_sax_handler Class Reference	107
10.15.1 Detailed Description	107
10.15.2 Member Data Documentation	107
10.16irbe_cli.list_published_objects_elt Class Reference	107
10.16.1 Detailed Description	108
10.16.2 Member Data Documentation	108
10.17irbe_cli.manifest_elt Class Reference	108
10.17.1 Detailed Description	108
10.18irbe_cli.parent_elt Class Reference	108
10.18.1 Detailed Description	108
10.19irbe_cli.publication_cms_msg Class Reference	109
10.19.1 Detailed Description	109
10.19.2 Member Data Documentation	109
10.20irbe_cli.publication_msg Class Reference	109
10.20.1 Detailed Description	109
10.20.2 Member Data Documentation	110
10.21irbe_cli.publication_sax_handler Class Reference	110
10.21.1 Detailed Description	110
10.21.2 Member Data Documentation	110
10.22irbe_cli.reply_elt_mixin Class Reference	111
10.22.1 Detailed Description	111
10.22.2 Member Function Documentation	111
10.22.3 Member Data Documentation	111
10.23irbe_cli.report_error_elt Class Reference	112
10.23.1 Detailed Description	112
10.24irbe_cli.repository_elt Class Reference	112

10.24.1 Detailed Description	112
10.25irbe_cli.roa_elt Class Reference	112
10.25.1 Detailed Description	112
10.26irbe_cli.self_elt Class Reference	113
10.26.1 Detailed Description	113
10.27irbe_cli.UsageWrapper Class Reference	113
10.27.1 Detailed Description	113
10.27.2 Member Function Documentation	113
10.28long Class Reference	114
10.29object Class Reference	114
10.30pubd.pubd_context Class Reference	114
10.30.1 Detailed Description	115
10.30.2 Member Function Documentation	115
10.30.3 Member Data Documentation	116
10.31datetime Class Reference	118
10.32timedelta Class Reference	118
10.33rootd.cms_msg Class Reference	118
10.33.1 Detailed Description	118
10.33.2 Member Data Documentation	118
10.34rootd.issue_pdu Class Reference	119
10.34.1 Detailed Description	119
10.34.2 Member Function Documentation	119
10.35rootd.list_pdu Class Reference	119
10.35.1 Detailed Description	119
10.35.2 Member Function Documentation	120
10.36rootd.message_pdu Class Reference	120
10.36.1 Detailed Description	120
10.36.2 Member Function Documentation	120
10.36.3 Member Data Documentation	121
10.37rootd.revoke_pdu Class Reference	121
10.37.1 Detailed Description	121

10.37.2 Member Function Documentation	122
10.38rootd.sax_handler Class Reference	122
10.38.1 Detailed Description	122
10.38.2 Member Data Documentation	122
10.39rpki.async.iterator Class Reference	122
10.39.1 Detailed Description	123
10.39.2 Member Function Documentation	123
10.39.3 Member Data Documentation	124
10.40rpki.async.sync_wrapper Class Reference	125
10.40.1 Detailed Description	125
10.40.2 Member Function Documentation	126
10.40.3 Member Data Documentation	126
10.41rpki.async.timer Class Reference	127
10.41.1 Detailed Description	128
10.41.2 Member Function Documentation	128
10.41.3 Member Data Documentation	131
10.42rpki.config.parser Class Reference	131
10.42.1 Detailed Description	132
10.42.2 Member Function Documentation	132
10.42.3 Member Data Documentation	134
10.43rpki.exceptions.BadClassNameSyntax Class Reference	134
10.43.1 Detailed Description	134
10.44rpki.exceptions.BadClientURL Class Reference	135
10.44.1 Detailed Description	135
10.45rpki.exceptions.BadContactURL Class Reference	135
10.45.1 Detailed Description	135
10.46rpki.exceptions.BadExtension Class Reference	135
10.46.1 Detailed Description	135
10.47rpki.exceptions.BadIRDBReply Class Reference	136
10.47.1 Detailed Description	136
10.48rpki.exceptions.BadIssueResponse Class Reference	136

10.48.1 Detailed Description	136
10.49rpki.exceptions.BadPKCS10 Class Reference	136
10.49.1 Detailed Description	136
10.50rpki.exceptions.BadPublicationReply Class Reference	137
10.50.1 Detailed Description	137
10.51rpki.exceptions.BadQuery Class Reference	137
10.51.1 Detailed Description	137
10.52rpki.exceptions.BadSender Class Reference	137
10.52.1 Detailed Description	137
10.53rpki.exceptions.BadStatusCode Class Reference	138
10.53.1 Detailed Description	138
10.54rpki.exceptions.BadURISyntax Class Reference	138
10.54.1 Detailed Description	138
10.55rpki.exceptions.BSCNotFound Class Reference	138
10.55.1 Detailed Description	138
10.56rpki.exceptions.BSCNotReady Class Reference	139
10.56.1 Detailed Description	139
10.57rpki.exceptions.ChildNotFound Class Reference	139
10.57.1 Detailed Description	139
10.58rpki.exceptions.ClassNameMismatch Class Reference	139
10.58.1 Detailed Description	139
10.59rpki.exceptions.ClassNameUnknown Class Reference	140
10.59.1 Detailed Description	140
10.60rpki.exceptions.ClientNotFound Class Reference	140
10.60.1 Detailed Description	140
10.61rpki.exceptions.CMSCRLNotSet Class Reference	140
10.61.1 Detailed Description	140
10.62rpki.exceptions.CMSVerificationFailed Class Reference	141
10.62.1 Detailed Description	141
10.63rpki.exceptions.DBConsistencyError Class Reference	141
10.63.1 Detailed Description	141

10.64rpki.exceptions.DERObjectConversionError Class Reference	141
10.64.1 Detailed Description	141
10.65rpki.exceptions.DuplicateObject Class Reference	142
10.65.1 Detailed Description	142
10.66rpki.exceptions.EmptyPEM Class Reference	142
10.66.1 Detailed Description	142
10.67rpki.exceptions.EmptyROAPrefixList Class Reference	142
10.67.1 Detailed Description	142
10.68rpki.exceptions.ForbiddenURI Class Reference	143
10.68.1 Detailed Description	143
10.69rpki.exceptions.HandleTranslationError Class Reference	143
10.69.1 Detailed Description	143
10.70rpki.exceptions.HTTPRequestFailed Class Reference	143
10.70.1 Detailed Description	143
10.71rpki.exceptions.HTTPSBadVersion Class Reference	144
10.71.1 Detailed Description	144
10.72rpki.exceptions.HTTPSClientAborted Class Reference	144
10.72.1 Detailed Description	144
10.73rpki.exceptions.HTTPSUnexpectedState Class Reference	144
10.73.1 Detailed Description	144
10.74rpki.exceptions.MissingCMSCRL Class Reference	145
10.74.1 Detailed Description	145
10.75rpki.exceptions.MissingCMSEECert Class Reference	145
10.75.1 Detailed Description	145
10.76rpki.exceptions.MultipleTLSEECert Class Reference	145
10.76.1 Detailed Description	145
10.77rpki.exceptions.MustBePrefix Class Reference	146
10.77.1 Detailed Description	146
10.78rpki.exceptions.NoActiveCA Class Reference	146
10.78.1 Detailed Description	146
10.79rpki.exceptions.NoCoveringCertForROA Class Reference	146

10.79.1 Detailed Description	146
10.80rpki.exceptions.NoObjectAtURI Class Reference	147
10.80.1 Detailed Description	147
10.81rpki.exceptions.NotACertificateChain Class Reference	147
10.81.1 Detailed Description	147
10.82rpki.exceptions.NotFound Class Reference	147
10.82.1 Detailed Description	147
10.83rpki.exceptions.NotImplementedYet Class Reference	148
10.83.1 Detailed Description	148
10.84rpki.exceptions.NotInDatabase Class Reference	148
10.84.1 Detailed Description	148
10.85rpki.exceptions.ReceivedTLSCACert Class Reference	148
10.85.1 Detailed Description	148
10.86rpki.exceptions.RPKI_Exception Class Reference	149
10.86.1 Detailed Description	149
10.87rpki.exceptions.ServerShuttingDown Class Reference	149
10.87.1 Detailed Description	150
10.88rpki.exceptions.SKIMismatch Class Reference	150
10.88.1 Detailed Description	150
10.89rpki.exceptions.SubprocessError Class Reference	150
10.89.1 Detailed Description	150
10.90rpki.exceptions.TLSValidationError Class Reference	150
10.90.1 Detailed Description	151
10.91rpki.exceptions.UnexpectedCMSCerts Class Reference	151
10.91.1 Detailed Description	151
10.92rpki.exceptions.UnexpectedCMSCRLs Class Reference	151
10.92.1 Detailed Description	151
10.93rpki.exceptions.UnparsableCMSDER Class Reference	151
10.93.1 Detailed Description	152
10.94rpki.exceptions.UpstreamError Class Reference	152
10.94.1 Detailed Description	152

10.95rpki.exceptions.WrongEContentType Class Reference	152
10.95.1 Detailed Description	152
10.96rpki.https.http_client Class Reference	152
10.96.1 Detailed Description	153
10.96.2 Member Function Documentation	153
10.96.3 Member Data Documentation	155
10.97rpki.https.http_listener Class Reference	157
10.97.1 Detailed Description	157
10.97.2 Member Function Documentation	157
10.97.3 Member Data Documentation	158
10.98rpki.https.http_message Class Reference	159
10.98.1 Detailed Description	159
10.98.2 Member Function Documentation	160
10.98.3 Member Data Documentation	161
10.99rpki.https.http_queue Class Reference	161
10.99.1 Detailed Description	162
10.99.2 Member Function Documentation	162
10.99.3 Member Data Documentation	163
10.100rpki.https.http_request Class Reference	164
10.100.1 Detailed Description	164
10.100.2 Member Function Documentation	165
10.100.3 Member Data Documentation	165
10.101rpki.https.http_response Class Reference	166
10.101.1 Detailed Description	166
10.101.2 Member Function Documentation	166
10.101.3 Member Data Documentation	167
10.102rpki.https.http_server Class Reference	167
10.102.1 Detailed Description	168
10.102.2 Member Function Documentation	168
10.102.3 Member Data Documentation	169
10.103rpki.https.http_stream Class Reference	170

10.103.	Detailed Description	171
10.103.	Member Function Documentation	172
10.103.	Member Data Documentation	175
10.104.	ipki.ipaddrs.v4addr Class Reference	176
10.104.	Detailed Description	176
10.104.	Member Function Documentation	177
10.104.	Member Data Documentation	177
10.105.	ipki.ipaddrs.v6addr Class Reference	178
10.105.	Detailed Description	178
10.105.	Member Function Documentation	178
10.105.	Member Data Documentation	179
10.106.	ipki.left_right.bsc_elt Class Reference	179
10.106.	Detailed Description	180
10.106.	Member Function Documentation	180
10.106.	Member Data Documentation	181
10.107.	ipki.left_right.child_elt Class Reference	183
10.107.	Detailed Description	184
10.107.	Member Function Documentation	184
10.107.	Member Data Documentation	186
10.108.	ipki.left_right.cms_msg Class Reference	188
10.108.	Detailed Description	188
10.108.	Member Data Documentation	188
10.109.	ipki.left_right.data_elt Class Reference	189
10.109.	Detailed Description	189
10.109.	Member Function Documentation	189
10.109.	Member Data Documentation	191
10.110.	ipki.left_right.left_right_namespace Class Reference	192
10.110.	Detailed Description	192
10.110.	Member Data Documentation	192
10.111.	ipki.left_right.list_published_objects_elt Class Reference	193
10.111.	Detailed Description	193

10.111.2	Member Function Documentation	193
10.111.3	Member Data Documentation	194
10.111	rpki.left_right.list_resources_elt Class Reference	195
10.112.1	Detailed Description	195
10.112.2	Member Function Documentation	195
10.112.3	Member Data Documentation	196
10.112	rpki.left_right.list_roa_requests_elt Class Reference	197
10.113.1	Detailed Description	198
10.113.2	Member Function Documentation	198
10.113.3	Member Data Documentation	198
10.114	rpki.left_right.msg Class Reference	199
10.114.1	Detailed Description	199
10.114.2	Member Function Documentation	199
10.114.3	Member Data Documentation	200
10.115	rpki.left_right.parent_elt Class Reference	200
10.115.1	Detailed Description	201
10.115.2	Member Function Documentation	201
10.115.3	Member Data Documentation	203
10.116	rpki.left_right.report_error_elt Class Reference	205
10.116.1	Detailed Description	206
10.116.2	Member Function Documentation	206
10.116.3	Member Data Documentation	206
10.117	rpki.left_right.repository_elt Class Reference	207
10.117.1	Detailed Description	208
10.117.2	Member Function Documentation	208
10.117.3	Member Data Documentation	209
10.118	rpki.left_right.sax_handler Class Reference	211
10.118.1	Detailed Description	211
10.118.2	Member Data Documentation	211
10.119	rpki.left_right.self_elt Class Reference	212
10.119.1	Detailed Description	213

10.119.2	Member Function Documentation	213
10.119.3	Member Data Documentation	217
10.120	rpki.log.logger Class Reference	219
10.120.1	Detailed Description	220
10.120.2	Member Function Documentation	220
10.120.3	Member Data Documentation	220
10.121	rpki.manifest.FileAndHash Class Reference	220
10.121.1	Detailed Description	221
10.121.2	Member Function Documentation	221
10.121.3	Member Data Documentation	221
10.122	rpki.manifest.FilesAndHashes Class Reference	221
10.122.1	Detailed Description	221
10.122.2	Member Function Documentation	222
10.123	rpki.manifest.Manifest Class Reference	222
10.123.1	Detailed Description	222
10.123.2	Member Function Documentation	222
10.123.3	Member Data Documentation	223
10.124	rpki.publication.certificate_elt Class Reference	224
10.124.1	Detailed Description	224
10.124.2	Member Data Documentation	224
10.125	rpki.publication.client_elt Class Reference	225
10.125.1	Detailed Description	225
10.125.2	Member Function Documentation	225
10.125.3	Member Data Documentation	227
10.126	rpki.publication.cms_msg Class Reference	228
10.126.1	Detailed Description	228
10.126.2	Member Data Documentation	229
10.127	rpki.publication.config_elt Class Reference	229
10.127.1	Detailed Description	230
10.127.2	Member Function Documentation	230
10.127.3	Member Data Documentation	231

10.128	rpkim.publication.control_elt Class Reference	232
10.128	Detailed Description	232
10.128	Member Function Documentation	233
10.129	rpkim.publication.crl_elt Class Reference	233
10.129	Detailed Description	233
10.129	Member Data Documentation	233
10.130	rpkim.publication.manifest_elt Class Reference	234
10.130	Detailed Description	234
10.130	Member Data Documentation	234
10.131	rpkim.publication.msg Class Reference	235
10.131	Detailed Description	235
10.131	Member Function Documentation	235
10.131	Member Data Documentation	236
10.132	rpkim.publication.publication_namespace Class Reference	236
10.132	Detailed Description	236
10.132	Member Data Documentation	237
10.133	rpkim.publication.publication_object_elt Class Reference	237
10.133	Detailed Description	238
10.133	Member Function Documentation	238
10.133	Member Data Documentation	240
10.134	rpkim.publication.report_error_elt Class Reference	240
10.134	Detailed Description	241
10.134	Member Function Documentation	241
10.134	Member Data Documentation	242
10.135	rpkim.publication.roa_elt Class Reference	243
10.135	Detailed Description	243
10.135	Member Data Documentation	243
10.136	rpkim.publication.sax_handler Class Reference	244
10.136	Detailed Description	244
10.136	Member Data Documentation	244
10.137	rpkim.resource_set.resource_bag Class Reference	245

10.137.	Detailed Description	245
10.137.	Member Function Documentation	246
10.137.	Member Data Documentation	247
10.138.	rpki.resource_set.resource_range Class Reference	248
10.138.	Detailed Description	249
10.138.	Member Function Documentation	249
10.138.	Member Data Documentation	249
10.139.	rpki.resource_set.resource_range_as Class Reference	250
10.139.	Detailed Description	250
10.139.	Member Function Documentation	250
10.139.	Member Data Documentation	251
10.140.	rpki.resource_set.resource_range_ip Class Reference	251
10.140.	Detailed Description	252
10.140.	Member Function Documentation	252
10.141.	rpki.resource_set.resource_range_ipv4 Class Reference	253
10.141.	Detailed Description	253
10.141.	Member Data Documentation	253
10.142.	rpki.resource_set.resource_range_ipv6 Class Reference	254
10.142.	Detailed Description	254
10.142.	Member Data Documentation	254
10.143.	rpki.resource_set.resource_set Class Reference	254
10.143.	Detailed Description	255
10.143.	Member Function Documentation	255
10.143.	Member Data Documentation	258
10.144.	rpki.resource_set.resource_set_as Class Reference	258
10.144.	Detailed Description	258
10.144.	Member Function Documentation	259
10.144.	Member Data Documentation	259
10.145.	rpki.resource_set.resource_set_ip Class Reference	260
10.145.	Detailed Description	260
10.145.	Member Function Documentation	260

10.145.	Member Data Documentation	261
10.146.	pk resource_set.resource_set_ipv4 Class Reference	261
10.146.	Detailed Description	262
10.146.	Member Data Documentation	262
10.147.	pk resource_set.resource_set_ipv6 Class Reference	262
10.147.	Detailed Description	263
10.147.	Member Data Documentation	263
10.148.	pk resource_set.roa_prefix Class Reference	263
10.148.	Detailed Description	264
10.148.	Member Function Documentation	264
10.148.	Member Data Documentation	266
10.149.	pk resource_set.roa_prefix_ipv4 Class Reference	266
10.149.	Detailed Description	266
10.149.	Member Data Documentation	267
10.150.	pk resource_set.roa_prefix_ipv6 Class Reference	267
10.150.	Detailed Description	267
10.150.	Member Data Documentation	267
10.151.	pk resource_set.roa_prefix_set Class Reference	268
10.151.	Detailed Description	268
10.151.	Member Function Documentation	268
10.152.	pk resource_set.roa_prefix_set_ipv4 Class Reference	270
10.152.	Detailed Description	270
10.152.	Member Data Documentation	270
10.153.	pk resource_set.roa_prefix_set_ipv6 Class Reference	271
10.153.	Detailed Description	271
10.153.	Member Data Documentation	271
10.154.	pk roa.ROAIPAddress Class Reference	272
10.154.	Detailed Description	272
10.154.	Member Function Documentation	272
10.154.	Member Data Documentation	272
10.155.	pk roa.ROAIPAddresses Class Reference	273

10.155.Detailed Description	273
10.155.Member Function Documentation	273
10.156rpki.roa.ROAIPAddressFamilies Class Reference	273
10.156.Detailed Description	273
10.156.Member Function Documentation	274
10.157rpki.roa.ROAIPAddressFamily Class Reference	274
10.157.Detailed Description	274
10.157.Member Function Documentation	274
10.157.Member Data Documentation	275
10.158rpki.roa.RouteOriginAttestation Class Reference	275
10.158.Detailed Description	275
10.158.Member Function Documentation	275
10.158.Member Data Documentation	276
10.159rpki.rpki_engine.ca_detail_obj Class Reference	276
10.159.Detailed Description	277
10.159.Member Function Documentation	278
10.159.Member Data Documentation	282
10.160rpki.rpki_engine.ca_obj Class Reference	284
10.160.Detailed Description	285
10.160.Member Function Documentation	285
10.160.Member Data Documentation	289
10.161rpki.rpki_engine.child_cert_obj Class Reference	290
10.161.Detailed Description	291
10.161.Member Function Documentation	291
10.161.Member Data Documentation	293
10.162rpki.rpki_engine.revoked_cert_obj Class Reference	294
10.162.Detailed Description	294
10.162.Member Function Documentation	295
10.162.Member Data Documentation	295
10.163rpki.rpki_engine.roa_obj Class Reference	296
10.163.Detailed Description	297

10.163.	Member Function Documentation	297
10.163.	Member Data Documentation	300
10.164.	rpki.rpki_engine.rpkid_context Class Reference	302
10.164.	Detailed Description	303
10.164.	Member Function Documentation	303
10.164.	Member Data Documentation	305
10.165.	rpki.sql.session Class Reference	308
10.165.	Detailed Description	309
10.165.	Member Function Documentation	309
10.165.	Member Data Documentation	311
10.166.	rpki.sql.sql_persistent Class Reference	312
10.166.	Detailed Description	313
10.166.	Member Function Documentation	313
10.166.	Member Data Documentation	317
10.167.	rpki.sql.template Class Reference	318
10.167.	Detailed Description	318
10.167.	Member Function Documentation	318
10.167.	Member Data Documentation	318
10.168.	rpki.sundial.datetime Class Reference	320
10.168.	Detailed Description	320
10.168.	Member Function Documentation	321
10.168.	Member Data Documentation	324
10.169.	rpki.sundial.timedelta Class Reference	324
10.169.	Detailed Description	325
10.169.	Member Function Documentation	325
10.169.	Member Data Documentation	328
10.170.	rpki.up_down.base_elt Class Reference	328
10.170.	Detailed Description	329
10.170.	Member Function Documentation	329
10.171.	rpki.up_down.certificate_elt Class Reference	330
10.171.	Detailed Description	331

10.171.2	Member Function Documentation	331
10.171.3	Member Data Documentation	332
10.172	pkc.up_down.class_elt Class Reference	333
10.172.1	Detailed Description	333
10.172.2	Member Function Documentation	333
10.172.3	Member Data Documentation	335
10.173	pkc.up_down.class_response_syntax Class Reference	336
10.173.1	Detailed Description	336
10.173.2	Member Function Documentation	336
10.173.3	Member Data Documentation	337
10.174	pkc.up_down.cms_msg Class Reference	337
10.174.1	Detailed Description	338
10.174.2	Member Data Documentation	338
10.175	pkc.up_down.error_response_pdu Class Reference	338
10.175.1	Detailed Description	339
10.175.2	Member Function Documentation	339
10.175.3	Member Data Documentation	340
10.176	pkc.up_down.issue_pdu Class Reference	341
10.176.1	Detailed Description	342
10.176.2	Member Function Documentation	342
10.176.3	Member Data Documentation	343
10.177	pkc.up_down.issue_response_pdu Class Reference	344
10.177.1	Detailed Description	344
10.177.2	Member Function Documentation	344
10.178	pkc.up_down.list_pdu Class Reference	344
10.178.1	Detailed Description	345
10.178.2	Member Function Documentation	345
10.179	pkc.up_down.list_response_pdu Class Reference	346
10.179.1	Detailed Description	346
10.180	pkc.up_down.message_pdu Class Reference	346
10.180.1	Detailed Description	347

10.180.	Member Function Documentation	347
10.180.	Member Data Documentation	348
10.181.	pkix.up_down.multi_uri Class Reference	350
10.181.	Detailed Description	350
10.181.	Member Function Documentation	350
10.182.	pkix.up_down.revoke_pdu Class Reference	351
10.182.	Detailed Description	351
10.182.	Member Function Documentation	351
10.182.	Member Data Documentation	352
10.183.	pkix.up_down.revoke_response_pdu Class Reference	352
10.183.	Detailed Description	353
10.184.	pkix.up_down.revoke_syntax Class Reference	353
10.184.	Detailed Description	353
10.184.	Member Function Documentation	353
10.184.	Member Data Documentation	354
10.185.	pkix.up_down.sax_handler Class Reference	354
10.185.	Detailed Description	354
10.185.	Member Data Documentation	355
10.186.	pkix.x509.CMS_object Class Reference	355
10.186.	Detailed Description	356
10.186.	Member Function Documentation	357
10.186.	Member Data Documentation	358
10.187.	pkix.x509.CRL Class Reference	360
10.187.	Detailed Description	361
10.187.	Member Function Documentation	361
10.187.	Member Data Documentation	363
10.188.	pkix.x509.DER_CMS_object Class Reference	364
10.188.	Detailed Description	364
10.188.	Member Function Documentation	364
10.188.	Member Data Documentation	365
10.189.	pkix.x509.DER_object Class Reference	365

10.189.Detailed Description	366
10.189.2Member Function Documentation	366
10.189.3Member Data Documentation	371
10.190pkix509.PEM_converter Class Reference	372
10.190.Detailed Description	372
10.190.2Member Function Documentation	373
10.190.3Member Data Documentation	373
10.191pkix509.PKCS10 Class Reference	374
10.191.Detailed Description	374
10.191.2Member Function Documentation	375
10.191.3Member Data Documentation	376
10.192pkix509.ROA Class Reference	377
10.192.Detailed Description	377
10.192.2Member Function Documentation	377
10.192.3Member Data Documentation	378
10.193pkix509.RSA Class Reference	378
10.193.Detailed Description	379
10.193.2Member Function Documentation	379
10.193.3Member Data Documentation	380
10.194pkix509.RSAPublic Class Reference	381
10.194.Detailed Description	382
10.194.2Member Function Documentation	382
10.194.3Member Data Documentation	383
10.195pkix509.SignedManifest Class Reference	383
10.195.Detailed Description	384
10.195.2Member Function Documentation	384
10.195.3Member Data Documentation	385
10.196pkix509.X509 Class Reference	385
10.196.Detailed Description	386
10.196.2Member Function Documentation	387
10.196.3Member Data Documentation	389

10.197	rpki.x509.XML_CMS_object Class Reference	390
10.197.1	Detailed Description	391
10.197.2	Member Function Documentation	391
10.197.3	Member Data Documentation	393
10.198	rpki.xml_utils.base_elt Class Reference	393
10.198.1	Detailed Description	394
10.198.2	Member Function Documentation	394
10.198.3	Member Data Documentation	396
10.199	rpki.xml_utils.data_elt Class Reference	397
10.199.1	Detailed Description	398
10.199.2	Member Function Documentation	398
10.200	rpki.xml_utils.msg Class Reference	401
10.200.1	Detailed Description	402
10.200.2	Member Function Documentation	402
10.200.3	Member Data Documentation	403
10.201	rpki.xml_utils.sax_handler Class Reference	404
10.201.1	Detailed Description	404
10.201.2	Member Function Documentation	405
10.201.3	Member Data Documentation	407
10.202	rpki.xml_utils.text_elt Class Reference	407
10.202.1	Detailed Description	408
10.202.2	Member Function Documentation	408
10.202.3	Member Data Documentation	408
10.203	Sequence Class Reference	409
10.204	SequenceOf Class Reference	409
10.205	TextWrapper Class Reference	409
10.206	ContentHandler Class Reference	409
11	File Documentation	409
11.1	__init__.py File Reference	409
11.2	async.py File Reference	410

11.3 config.py File Reference	410
11.4 exceptions.py File Reference	410
11.5 https.py File Reference	412
11.6 ipaddrs.py File Reference	413
11.7 irbe_cli.py File Reference	413
11.8 irdbd.py File Reference	414
11.9 left_right.py File Reference	415
11.10log.py File Reference	416
11.11manifest.py File Reference	417
11.12oids.py File Reference	417
11.13pubd.py File Reference	417
11.14publication.py File Reference	418
11.15relaxng.py File Reference	418
11.16resource_set.py File Reference	419
11.17roa.py File Reference	420
11.18rootd.py File Reference	420
11.19rpki_engine.py File Reference	422
11.20rpkid.py File Reference	422
11.21sql.py File Reference	422
11.22sundial.py File Reference	423
11.23up_down.py File Reference	423
11.24x509.py File Reference	424
11.25xml_utils.py File Reference	424

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, design documents, a text mirror of portions of APNIC's Wiki, etc.

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

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

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

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

- The [installation instructions](#)
- The [operation instructions](#)
- A description of the [left-right protocol](#)
- A description of the [publication protocol](#)
- A description of the [BPKI model](#) used to secure the up-down, left-right, and publication protocols
- A description of the several [SQL database schemas](#)
- Some suggestions for [further reading](#)

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

2 Further Reading

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

- [The rcynic validation tool](#)
- [A live sample of rcynic's summary output](#)
- [APNIC's Wiki](#)
- [APNIC's project Trac instance](#)

3 Installation Guide

Preliminary installation instructions for [rpkid](#) et al.

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

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

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

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

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

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

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

The next step is to build the OpenSSL and POW binaries. At present the OpenSSL code is just a snapshot of the OpenSSL development sources, compiled with special options to enable RFC 3779 support that ISC wrote under previous contract to ARIN.

The POW (Python OpenSSL Wrapper) library is an extended copy of the stock POW release.

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

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

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

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

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

At this point, you should have all the necessary software installed. You will probably want to test it. All tests should be run from the `rpkid/` directory. The test suite requires a few more external packages, only one of which is Python code.

- <http://pyyaml.org/>. `testpoke.py` (an up-down protocol command line test client) and `testbed.py` (a test harness) use PyYAML.
 - FreeBSD: `/usr/ports/devel/py-yaml`
 - Ubuntu: `python-yaml`
- <http://xmlsoft.org/XSLT/>. Some of the test code uses `xsltproc`, from the Gnome LibXSLT package.
 - FreeBSD: `/usr/ports/textproc/libxslt`
 - Ubuntu: `xsltproc`
- <http://w3m.sourceforge.net/>. `testbed.py` uses `w3m` to display the summary output from `rcynic`. Nothing terrible will happen if `w3m` isn't available, `testbed.py` will just complain about it being missing and won't display `rcynic`'s output.
 - FreeBSD: `/usr/ports/www/w3m`
 - Ubuntu: `w3m`

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

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

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

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

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

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

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

4 Operation Guide

Preliminary operation instructions for [rpkid](#) et al.

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

Warning:

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

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

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

- `rpkid.py`: The main RPKI engine daemon.
- `pubd.py`: The `publication` engine daemon.
- `rootd.py`: A separate daemon for handling the root of an RPKI certificate tree. This is essentially a stripped down version of `rpkid` with no SQL database, no left-right protocol implementation, and only the parent side of the up-down protocol. It's separate because the root is a special case in several ways and it was simpler to keep the special cases out of the main daemon.
- `irdbd.py`: A sample implementation of an IR database daemon. `rpkid` calls into this to perform lookups via the left-right protocol.
- `irbe_cli.py`: A command-line client for the left-right control protocol.
- `cross_certify.py`: A BPKI cross-certification tool.
- `irbe-setup.py`: An example of a script to set up the mappings between the IRDB and `rpkid`'s own database, using the left-right control protocol.
- `cronjob.py`: A trivial HTTP client used to drive `rpkid` cron events.
- `testbed.py`: A test tool for running a collection of `rpkid` and `irdb` instances under common control, driven by a unified test script.
- `testpoke.py`: A simple client for the up-down protocol, mostly compatible with APNIC's `rpki_poke.pl` tool.

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

Basic operation consists of creating the appropriate MySQL databases, starting [rpkiid](#), [pubd](#), [rootd](#), and [irdbd](#), using the left-right control protocol to set up [rpkiid](#)'s internal state, and setting up a cron job to invoke [rpkiid](#)'s cron action at regular intervals. All other operations should occur either as a result of cron events or as a result of incoming left-right and up-down protocol requests.

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

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

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

All of the daemons use syslog. At present they all set LOG_PERROR, so all logging also goes to stderr.

4.1 rpkiid.py

[rpkiid](#) is the main RPKI engine daemon. Configuration of [rpkiid](#) is a two step process: a config file to bootstrap [rpkiid](#) to the point where it can speak using the [left-right protocol](#), followed by dynamic configuration via the left-right protocol. In production use the latter stage would be handled by the IRBE stub; for test and development purposes it's handled by the [irbe_cli.py](#) command line interface or by the [testbed.py](#) test framework.

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

The default config file is [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 `rpkid` traces back to this trust anchor.
- `rpkid-cert`: Name of file containing `rpkid`'s own BPKI EE certificate.
- `rpkid-key`: Name of file containing RSA key corresponding to `rpkid-cert`.
- `irbe-cert`: Name of file containing BPKI certificate used by IRBE when talking to `rpkid`.
- `irdb-cert`: Name of file containing BPKI certificate used by `irdbd`.
- `irdb-url`: Service URL for `irdbd`. Must be a `https://` URL.
- `server-host`: Hostname or IP address on which to listen for HTTPS connections. Current default is `INADDR_ANY` (IPv4 0.0.0.0); this will need to be hacked to support IPv6 for production.
- `server-port`: TCP port on which to listen for HTTPS connections.

4.2 pubd.py

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

`pubd` is separate from `rpkid` for two reasons:

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

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

Config file options:

- `sql-username`: Username to hand to MySQL when connecting to pubd's database.
- `sql-database`: MySQL's database name for pubd's database.
- `sql-password`: Password to hand to MySQL when connecting to pubd's database.
- `bpmi-ta`: Name of file containing master BPKI trust anchor for [pubd](#). All BPKI validation in [pubd](#) traces back to this trust anchor.
- `irbe-cert`: Name of file containing BPKI certificate used by IRBE when talking to [pubd](#).
- `pubd-cert`: Name of file containing BPKI certificate used by [pubd](#).
- `pubd-key`: Name of file containing RSA key corresponding to `pubd-cert`.
- `server-host`: Hostname or IP address on which to listen for HTTPS connections. Current default is INADDR_ANY (IPv4 0.0.0.0); this will need to be hacked to support IPv6 for production.
- `server-port`: TCP port on which to listen for HTTPS connections.
- `publication-base`: Path to base of filesystem tree where [pubd](#) should store publishable objects. Default is "publication/".

4.3 rootd.py

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

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

Config file options:

- `bpki-ta`: Name of file containing BPKI trust anchor. All BPKI certificate validation in `rootd` traces back to this trust anchor.
- `rootd-bpki-cert`: Name of file containing rootd's own BPKI certificate.
- `rootd-bpki-key`: Name of file containing RSA key corresponding to rootd-bpki-cert.
- `rootd-bpki-crl`: Name of file containing BPKI CRL that would cover rootd-bpki-cert had it been revoked.
- `child-bpki-cert`: Name of file containing BPKI certificate for rootd's one and only child (RPKI engine to which `rootd` issues an RPKI certificate).
- `server-host`: Hostname or IP address on which to listen for HTTPS connections. Default is localhost.
- `server-port`: TCP port on which to listen for HTTPS connections.
- `rpki-root-key`: Name of file containing RSA key to use in signing resource certificates.
- `rpki-root-cert`: Name of file containing self-signed root resource certificate corresponding to rpki-root-key.
- `rpki-root-dir`: Name of directory where `rootd` should write RPKI subject certificate, `manifest`, and CRL.
- `rpki-subject-cert`: Name of file that `rootd` should use to save the one and only certificate it issues. Default is "Subroot.cer".
- `rpki-root-crl`: Name of file to which `rootd` should save its RPKI CRL. Default is "Root.crl".
- `rpki-root-manifest`: Name of file to which `rootd` should save its RPKI `manifest`. Default is "Root.mnf".
- `rpki-subject-pkcs10`: Name of file that `rootd` should use when saving a copy of the received PKCS #10 request for a resource certificate. This is only used for debugging. Default is not to save the PKCS #10 request.

4.4 irdbd.py

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

[irdbd](#) requires a pre-populated database to represent the IR's customers. [irdbd](#) expects this database to use the SQL schema defined in `rpkid/irdbd.sql`. Once this database has been populated, the IRBE stub needs to create the appropriate objects in `rpkid`'s database via the control subset of the left-right protocol, and store the linkage IDs (foreign keys into `rpkid`'s database, basically) in the IRDB. The `irbe-setup.py` program shows an example of how to do this.

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

Config file options:

- `startup-message`: String to log on startup, useful when debugging a collection of [irdbd](#) instances at once.
- `sql-username`: Username to hand to MySQL when connecting to `irdbd`'s database.
- `sql-database`: MySQL's database name for `irdbd`'s database.
- `sql-password`: Password to hand to MySQL when connecting to `irdbd`'s database.
- `bpki-ta`: Name of file containing BPKI trust anchor. All BPKI certificate validation in [irdbd](#) traces back to this trust anchor.
- `irdbd-cert`: Name of file containing `irdbd`'s own BPKI certificate.
- `irdbd-key`: Name of file containing RSA key corresponding to `irdbd-cert`.
- `rpkid-cert`: Name of file containing certificate used the one and only by [rpkid](#) instance authorized to contact this [irdbd](#) instance.
- `https-url`: Service URL for [irdbd](#). Must be a `https://` URL.

4.5 irbe_cli.py

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

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

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

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

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

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

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

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

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

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

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

```
Usage:
```

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

```

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

# publication protocol:
certificate --action= --tag= --client_handle= --uri=
roa --action= --tag= --client_handle= --uri=
manifest --action= --tag= --client_handle= --uri=
client --action= --tag= --client_handle= --base_uri= --bpki_cert=
--bpki_glue=
config --action= --tag= --bpki_crl=
crl --action= --tag= --client_handle= --uri=

```

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

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

`-*_handle` options refer to [object](#) primary keys.

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

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

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

Config file options:

- `rpkid-bpki-ta`: Name of file containing BPKI trust anchor to use when authenticating messages from [rpkid](#).

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

4.6 cross_certify.py

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

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

4.7 irbe-setup.py config file

Warning:

`irbe-setup` is old code, not currently used, kept in case it is useful at some later date. It may not work properly or at all. If you don't understand what it does, you don't need it. You have been warned.

The default config file is `irbe.conf`, start `rpkid` with `"-c filename"` to choose a different config file. Most options are in the section `"[irbe_cli]"`, but a few are in the section `"[irbdb]"`. Certificates, keys, and trust anchors may be in either DER or PEM format.

Options in the `"[irbe_cli]"` section:

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

Options in the `"[irbdb]"` section:

- `sql-username`: Username to hand to MySQL when connecting to `irbdb`'s database.
- `sql-database`: MySQL's database name for `irbdb`'s database.
- `sql-password`: Password to hand to MySQL when connecting to `irbdb`'s database.

4.8 cronjob.py

This is a trivial program to trigger a cron run within `rpkid`. Once `rpkid` has been converted to the planned event-driven model, this function will be handled internally, but for now it has to be triggered by an external program. For pseudo-production use one would run this program under the system cron daemon. For scripted testing it happens to be useful to be able to control when cron cycles occur, so at the current stage of code development use of an external trigger is a useful feature.

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

Config file options:

- `bpki-ta`: Name of file containing BPKI trust anchor.
- `irbe-cert`: Name of file containing `cronjob.py`'s BPKI certificate.

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

4.9 testbed.py:

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

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

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

`testbed.conf` options:

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

The second configuration file is named `testbed.yaml` by default, run `testbed` with `"-y filename"` to change it. The YAML file contains multiple YAML "documents". The

first document describes the initial test layout and resource allocations, subsequent documents describe modifications to the initial allocations and other parameters. Resources listed in the initial layout are aggregated automatically, so that a node in the resource hierarchy automatically receives the resources it needs to issue whatever its children are listed as holding. Actions in the subsequent documents are modifications to the current resource set, modifications to validity dates or other non-resource parameters, or special commands like "sleep". The details are still evolving, but here's an example of current usage:

```
name:          RIR
valid_for:     2d
sia_base:      "rsync://wombat.invalid/"
kids:
- name: LIR0
  kids:
  - name: Alice
    ipv4: 192.0.2.1-192.0.2.33
    asn: 64533
---
- name: Alice
  valid_add: 10
---
- name: Alice
  add_as: 33
  valid_add: 2d
---
- name: Alice
  valid_sub: 2d
---
- name: Alice
  valid_for: 10d
```

This specifies an initial layout consisting of an RPKI engine named "RIR", with one child "LIR0", which in turn has one child "Alice". Alice has a set of assigned resources, and all resources in the system are initially set to be valid for two days from the time at which the test is started. The first subsequent document adds ten seconds to the validity interval for Alice's resources and makes no other modifications. The second subsequent document grants Alice additional resources and adds another two days to the validity interval for Alice's resources. The next document subtracts two days from the validity interval for Alice's resources. The final document sets the validity interval for Alice's resources to ten days.

Operators in subsequent (update) documents:

- `add_as`, `add_v4`, `add_v6`: These add ASN, IPv4, or IPv6 resources, respectively.
- `sub_as`, `sub_v4`, `sub_v6`: These subtract resources.
- `valid_until`: Set an absolute expiration date.

- `valid_for`: Set a relative expiration date.
- `valid_add, valid_sub`: Add to or subtract from validity interval.
- `sleep [interval]`: Sleep for specified interval, or until testbed receives a SIGALRM signal.

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

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

4.10 testpoke.py

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

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

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

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

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

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

Sample configuration file:

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

version: 1
posturl: https://localhost:4433/up-down/1
```

```
recipient-id: wombat
sender-id: "1"

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

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

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

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

5 Left-right protocol

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

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

5.1 Terminology

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

- *RPKI*: Resource PKI

5.2 initiated by the IRBE

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

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

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

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

5.2.1 <self/> object

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

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

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

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

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

- `use_hsm` (attribute): Whether to use a Hardware Signing Module. At present this option has no effect, as the implementation does not yet support HSMs.
- `crl_interval` (attribute): Positive integer representing the planned lifetime of an RPKI CRL for this `<self/>`, measured in seconds.
- `regen_margin` (attribute): Positive integer representing how long before expiration of an RPKI certificate a new one should be generated, measured in seconds. At present this only affects the one-off EE certificates associated with ROAs.
- `bpki_cert` (element): BPKI CA certificate for this `<self/>`. This is used as part of the certificate chain when validating incoming TLS and CMS messages, and should be the issuer of cross-certification BPKI certificates used in `<repository/>`, `<parent/>`, and `<child/>` objects. If the `bpki_glue` certificate is in use (below), the `bpki_cert` certificate should be issued by the `bpki_glue` certificate; otherwise, the `bpki_cert` certificate should be issued by the per-engine `bpki_ta` certificate.
- `bpki_glue` (element): Another BPKI CA certificate for this `<self/>`, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the `bpki_glue` certificate should be the issuer of the `bpki_cert` certificate and should be issued by the per-engine `bpki_ta` certificate; if not needed, the `bpki_glue` certificate should be left unset.

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

- `rekey`: Start a key rollover for every RPKI CA associated with every `<parent/>` object associated with this `<self/>` object. This is the first phase of a key rollover operation.
- `revoke`: Revoke any remaining certificates for any expired key associated with any RPKI CA for any `<parent/>` object associated with this `<self/>` object. This is the second (cleanup) phase for a key rollover operation; it's separate from the first phase to leave time for new RPKI certificates to propagate and be installed.
- `reissue`: Not implemented, may be removed from protocol. Original theory was that this operation would force reissuance of any object with a changed key,

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

- `run_now`: Force immediate processing for all tasks associated with this `<self/>` object that would ordinarily be performed under cron. Not currently implemented.
- `publish_world_now`: Force (re)publication of every publishable object for this `<self/>` object. Not currently implemented. Intended to aid in recovery if RPKI engine and publication engine somehow get out of sync.

5.2.2 `<bsc/>` object

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

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

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

- `signing_cert` (element): BPKI certificate to use when generating a signature.
- `signing_cert_crl` (element): CRL which would list `signing_cert` if it had been revoked.

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

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

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

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

- `hash_alg`: Cryptographic hash algorithm to use with this keypair. "sha256" is both the default and, at the moment, the only allowed value.
- `key_length`: Length in bits of the keypair to be generated. "2048" is both the default and, at the moment, the only allowed value.

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

5.2.3 `<parent/>` object

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

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

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

- `peer_contact_uri` (attribute): HTTPS URI used to contact this parent.
- `sia_base` (attribute): The leading portion of an rsync URI that the RPKI engine should use when composing the [publication](#) URI for objects issued by the RPKI certificate issued by this parent.
- `sender_name` (attribute): Sender name to use in the up-down protocol when talking to this parent. The RPKI engine doesn't really care what this value is, but other implementations of the up-down protocol do care.
- `recipient_name` (attribute): Recipient name to use in the up-down protocol when talking to this parent. The RPKI engine doesn't really care what this value is, but other implementations of the up-down protocol do care.

- `bpki_cms_cert` (element): BPKI CMS CA certificate for this `<parent/>`. This is used as part of the certificate chain when validating incoming CMS messages. If the `bpki_cms_glue` certificate is in use (below), the `bpki_cms_cert` certificate should be issued by the `bpki_cms_glue` certificate; otherwise, the `bpki_cms_cert` certificate should be issued by the `bpki_cert` certificate in the `<self/>` object.
- `bpki_cms_glue` (element): Another BPKI CMS CA certificate for this `<parent/>`, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the `bpki_cms_glue` certificate should be the issuer of the `bpki_cms_cert` certificate and should be issued by the `bpki_cert` certificate in the `<self/>` object; if not needed, the `bpki_cms_glue` certificate should be left unset.
- `bpki_https_cert` (element): BPKI HTTPS CA certificate for this `<parent/>`. This is like the `bpki_cms_cert` object, only used for validating incoming TLS messages rather than CMS.
- `bpki_https_glue` (element): Another BPKI HTTPS CA certificate for this `<parent/>`, usually not needed. This is like the `bpki_cms_glue` certificate, only used for validating incoming TLS messages rather than CMS.

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

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

5.2.4 `<child/>` object

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

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

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

- `bpki_cert` (element): BPKI CA certificate for this `<child/>`. This is used as part of the certificate chain when validating incoming TLS and CMS messages. If the `bpki_glue` certificate is in use (below), the `bpki_cert` certificate should be issued by the `bpki_glue` certificate; otherwise, the `bpki_cert` certificate should be issued by the `bpki_cert` certificate in the `<self/>` object.
- `bpki_glue` (element): Another BPKI CA certificate for this `<child/>`, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the `bpki_glue` certificate should be the issuer of the `bpki_cert` certificate and should be issued by the `bpki_cert` certificate in the `<self/>` object; if not needed, the `bpki_glue` certificate should be left unset.

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

- `reissue`: Not implemented, may be removed from protocol.

5.2.5 `<repository/>` object

The `<repository/>` object represents the RPKI engine's view of a particular [publication](#) repository used by the current `<self/>` object.

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

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

- `peer_contact_uri` (attribute): HTTPS URI used to contact this repository.
- `bpki_cms_cert` (element): BPKI CMS CA certificate for this `<repository/>`. This is used as part of the certificate chain when validating incoming CMS messages. If the `bpki_cms_glue` certificate is in use (below), the `bpki_cms_cert` certificate should be issued by the `bpki_cms_glue` certificate; otherwise, the `bpki_cms_cert` certificate should be issued by the `bpki_cert` certificate in the `<self/>` object.
- `bpki_cms_glue` (element): Another BPKI CMS CA certificate for this `<repository/>`, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the `bpki_cms_glue` certificate should be the issuer of the `bpki_cms_cert` certificate and should be issued by the `bpki_cert` certificate in the `<self/>` object; if not needed, the `bpki_cms_glue` certificate should be left unset.

- `bpki_https_cert` (element): BPKI HTTPS CA certificate for this `<repository/>`. This is like the `bpki_cms_cert` object, only used for validating incoming TLS messages rather than CMS.
- `bpki_cms_glue` (element): Another BPKI HTTPS CA certificate for this `<repository/>`, usually not needed. This is like the `bpki_cms_glue` certificate, only used for validating incoming TLS messages rather than CMS.

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

5.2.6 `<route_origin/>` object

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

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

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

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

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

- `asn` (attribute): Autonomous System Number (ASN) to place in the generated ROA. A single ROA can only grant authorization to a single ASN; multiple ASNs require multiple ROAs, thus multiple `<route_origin/>` objects.
- `ipv4` (attribute): List of IPv4 prefix and `maxLength` values, see below for format.
- `ipv6` (attribute): List of IPv6 prefix and `maxLength` values, see below for format.

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

- `suppress_publication`: Not implemented, may be removed from protocol.

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

ABNF for these address lists:

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

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

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

5.3 Operations initiated by the RPKI engine

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

5.3.1 <list_resources/> messages

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

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

- `valid_until`: A timestamp indicating the date and time at which certificates generated by the RPKI engine for these data should expire. The timestamp is

expressed as an XML `xsd:dateTime`, must be expressed in UTC, and must carry the "Z" suffix indicating UTC.

- `asn`: A list of autonomous sequence numbers, expressed as a comma-separated sequence of decimal integers with no whitespace.
- `ipv4`: A list of IPv4 address prefixes and ranges, expressed as a comma-separated list of prefixes and ranges with no whitespace. See below for format details.
- `ipv6`: A list of IPv6 address prefixes and ranges, expressed as a comma-separated list of prefixes and ranges with no whitespace. See below for format details.

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

5.4 Error handling

Error in this protocol are handled at two levels.

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

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

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

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

The error itself is conveyed in the `error_code` (attribute). The value of this attribute is a token indicating the specific error that occurred. At present this will be the name of

a Python exception; the production version of this protocol will nail down the allowed error tokens here, probably in the RelaxNG schema.

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

6 Publication protocol

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

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

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

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

6.1 Terminology

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

6.2 Publication control subprotocol

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

6.2.1 <config/> object

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

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

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

- `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.

6.2.2 <client/> object

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

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

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

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

6.3 Publication subprotocol

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

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

6.3.1 <certificate/> object

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

6.3.2 <crl/> object

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

6.3.3 <manifest/> object

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

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

6.3.4 <roa/> object

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

6.4 Error handling

Error in this protocol are handled at two levels.

Since all messages in this protocol are conveyed over HTTPS connections, basic errors are indicated via the HTTP response code. 4xx and 5xx responses indicate that

something bad happened. Errors that make it impossible to decode a query or encode a response are handled in this way.

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

`<report_error/>` messages only appear in replies, never in queries. The `<report_error/>` message can appear in both the control and [publication](#) subprotocols.

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

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

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

6.5 Additional access control considerations.

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

- In the case where parent and child are sharing a repository, we'd like to nest child under parent, because testing has demonstrated that even on relatively slow hardware the delays involved in setting up separate rsync connections tend to dominate synchronization time for relying parties.
- The repository operator might also want to do some checks to assure itself that what it's about to allow the RPKI engine to publish is not dangerous toxic waste.

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

In this case, one could argue that the publication server is responsible for preventing one of its clients (the child in the above description) from stomping on data published by another of its clients (the parent in the above description). This goes beyond the

basic access check and requires the publication server to determine whether the parent has given its consent for the child to publish under the parent. Since the RPKI certificate profile requires the child's publication point to be indicated in an SIA extension in a certificate issued by the parent to the child, the publication engine can infer this permission from the parent's issuance of a certificate to the child. Since, by definition, the parent also uses this publication server, this is an easy check, as the publication server should already have the parent's certificate available by the time it needs to check the child's certificate.

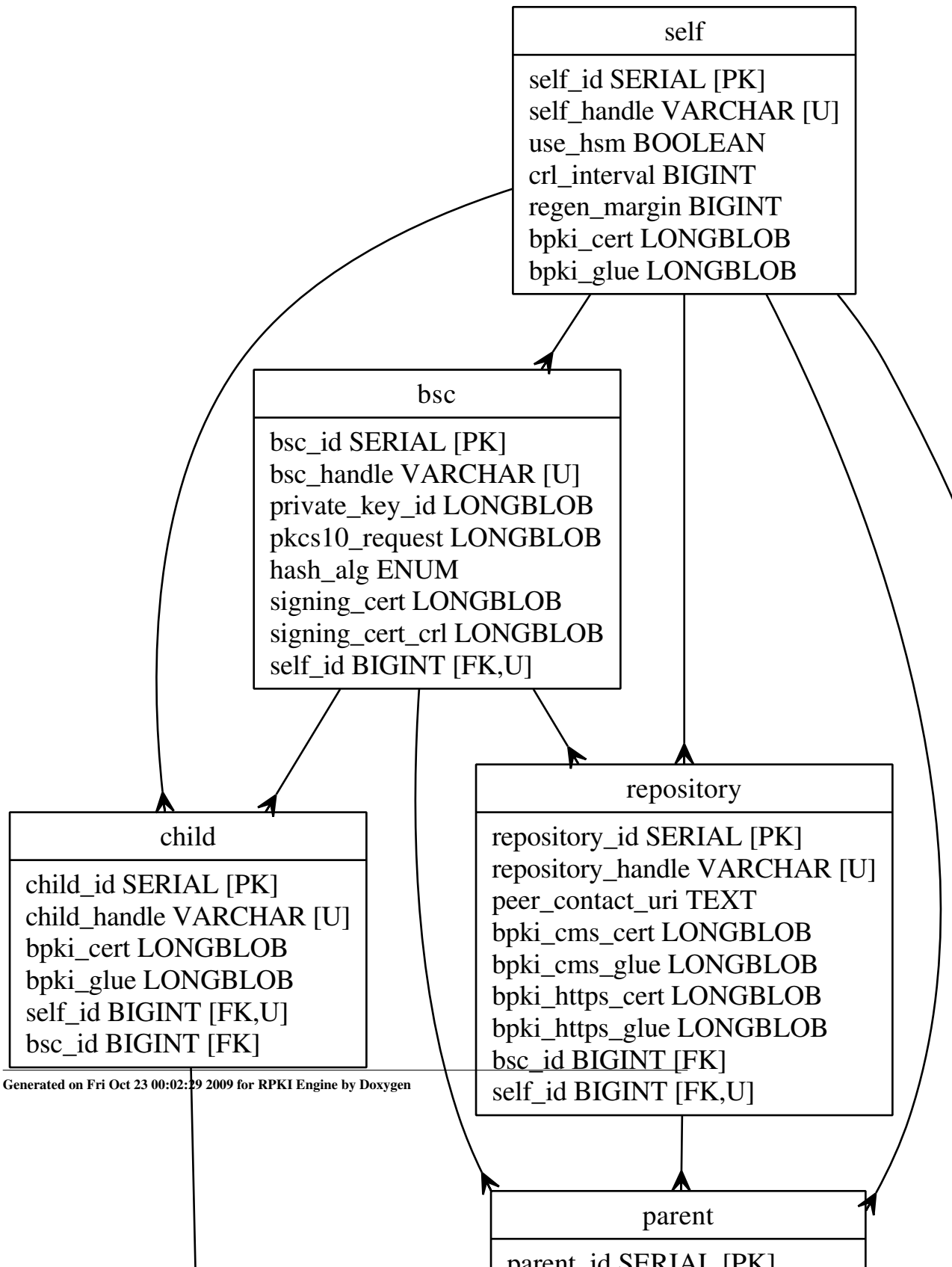
The previous paragraph only covers a "publish" action for a <certificate/> object. For "publish" actions on other objects, the publication server would need to trace permission back to the certificate issued by the parent; for "withdraw" actions, the publication server would have to perform the same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

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

7 SQL database schemas

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

7.1 rpkid SQL schema



```
-- $Id: rpkiid.sql 2781 2009-09-23 13:19:55Z 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.

-- 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 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,
    srl_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),
    FOREIGN KEY      (self_id) REFERENCES self (self_id),
    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,
    bpk_i_cert             LONGBLOB,
    bpk_i_glue             LONGBLOB,
    bsc_id                 BIGINT UNSIGNED NOT NULL,
    self_id               BIGINT UNSIGNED NOT NULL,
    PRIMARY KEY            (repository_id),
    FOREIGN KEY            (self_id) REFERENCES self (self_id),
    FOREIGN KEY            (bsc_id) REFERENCES bsc (bsc_id),
    UNIQUE                (self_id, repository_handle)
) ENGINE=InnoDB;

CREATE TABLE parent (
    parent_id             SERIAL NOT NULL,
    parent_handle         VARCHAR(255) NOT NULL,
    bpk_i_cms_cert        LONGBLOB,
    bpk_i_cms_glue        LONGBLOB,
    bpk_i_https_cert      LONGBLOB,
    bpk_i_https_glue      LONGBLOB,
    peer_contact_uri      TEXT,
    sia_base              TEXT,
    sender_name           TEXT,
    recipient_name        TEXT,
    self_id               BIGINT UNSIGNED NOT NULL,
    bsc_id               BIGINT UNSIGNED NOT NULL,
    repository_id         BIGINT UNSIGNED NOT NULL,
    PRIMARY KEY           (parent_id),
    FOREIGN KEY           (repository_id) REFERENCES repository (repository_id),
    FOREIGN KEY           (bsc_id) REFERENCES bsc (bsc_id),
    FOREIGN KEY           (self_id) REFERENCES self (self_id),
    UNIQUE                (self_id, parent_handle)
) ENGINE=InnoDB;

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

CREATE TABLE ca_detail (
    ca_detail_id          SERIAL NOT NULL,
    public_key            LONGBLOB,
    private_key_id        LONGBLOB,
    latest_crl            LONGBLOB,
    latest_ca_cert        LONGBLOB,

```

```

        manifest_private_key_id LONGBLOB,
        manifest_public_key     LONGBLOB,
        latest_manifest_cert     LONGBLOB,
        latest_manifest          LONGBLOB,
        state                    ENUM ('pending', 'active', 'deprecated', 'revoked') NOT NULL,
        ca_cert_uri              TEXT,
        ca_id                    BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY              (ca_detail_id),
        FOREIGN KEY              (ca_id) REFERENCES ca (ca_id)
    ) ENGINE=InnoDB;

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

CREATE TABLE child_cert (
    child_cert_id              SERIAL NOT NULL,
    cert                       LONGBLOB NOT NULL,
    ski                        TINYBLOB NOT NULL,
    child_id                   BIGINT UNSIGNED NOT NULL,
    ca_detail_id               BIGINT UNSIGNED NOT NULL,
    PRIMARY KEY                (child_cert_id),
    FOREIGN KEY                (ca_detail_id) REFERENCES ca_detail (ca_detail_id),
    FOREIGN KEY                (child_id) REFERENCES child (child_id)
) 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),
    FOREIGN KEY                (ca_detail_id) REFERENCES ca_detail (ca_detail_id)
) ENGINE=InnoDB;

CREATE TABLE roa (
    roa_id                     SERIAL NOT NULL,
    asn                        DECIMAL(24,0),
    cert                       LONGBLOB,
    roa                        LONGBLOB,
    self_id                    BIGINT UNSIGNED NOT NULL,
    ca_detail_id               BIGINT UNSIGNED NOT NULL,
    PRIMARY KEY                (roa_id),
    FOREIGN KEY                (self_id) REFERENCES self (self_id),
    FOREIGN KEY                (ca_detail_id) REFERENCES ca_detail (ca_detail_id)
) ENGINE=InnoDB;

```

```

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

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

```

7.2 pubd SQL Schema

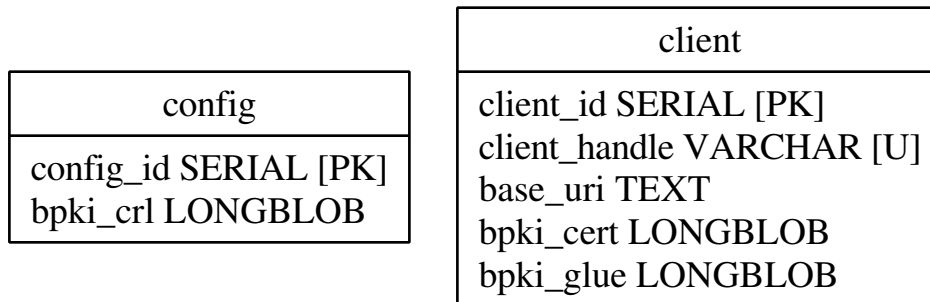


Figure 2: Diagram of pubd.sql

```

-- $Id: pubd.sql 2502 2009-06-08 03:56:26Z sra $

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

-- SQL objects needed by pubd.py.

-- The config table is weird because we're really only using it
-- to store one BPKI CRL, but putting this here lets us use a lot of

```



```
-- existing machinery and the alternatives are whacky in other ways.

DROP TABLE IF EXISTS client;
DROP TABLE IF EXISTS config;

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

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

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

7.3 irdbd SQL Schema

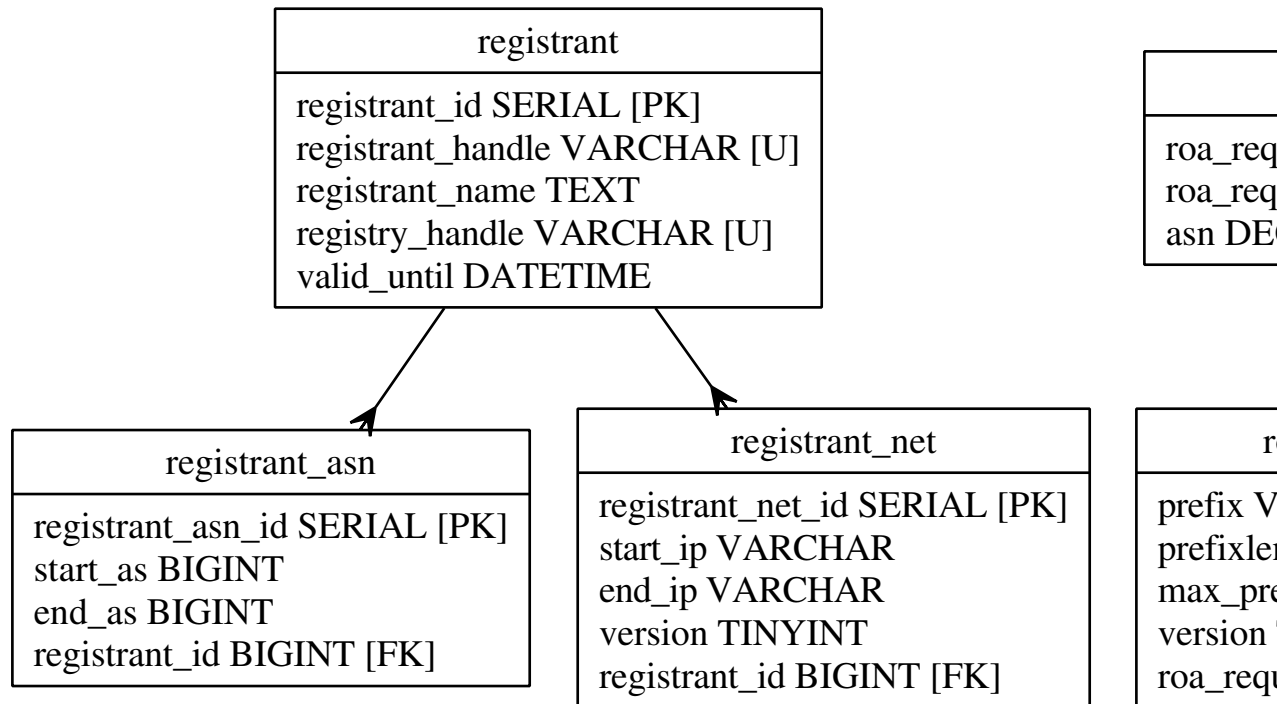


Figure 3: Diagram of irdbd.sql

```

-- $Id: irdbd.sql 2510 2009-06-09 20:25:16Z 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.

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

```

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

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

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

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

CREATE TABLE roa_request (
    roa_request_id         SERIAL NOT NULL,
    roa_request_handle      VARCHAR(255) NOT NULL,
    asn                    DECIMAL(24,0),
    PRIMARY KEY            (roa_request_id)
) ENGINE=InnoDB;

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

-- Local Variables:
```

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

8 BPKI model

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

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

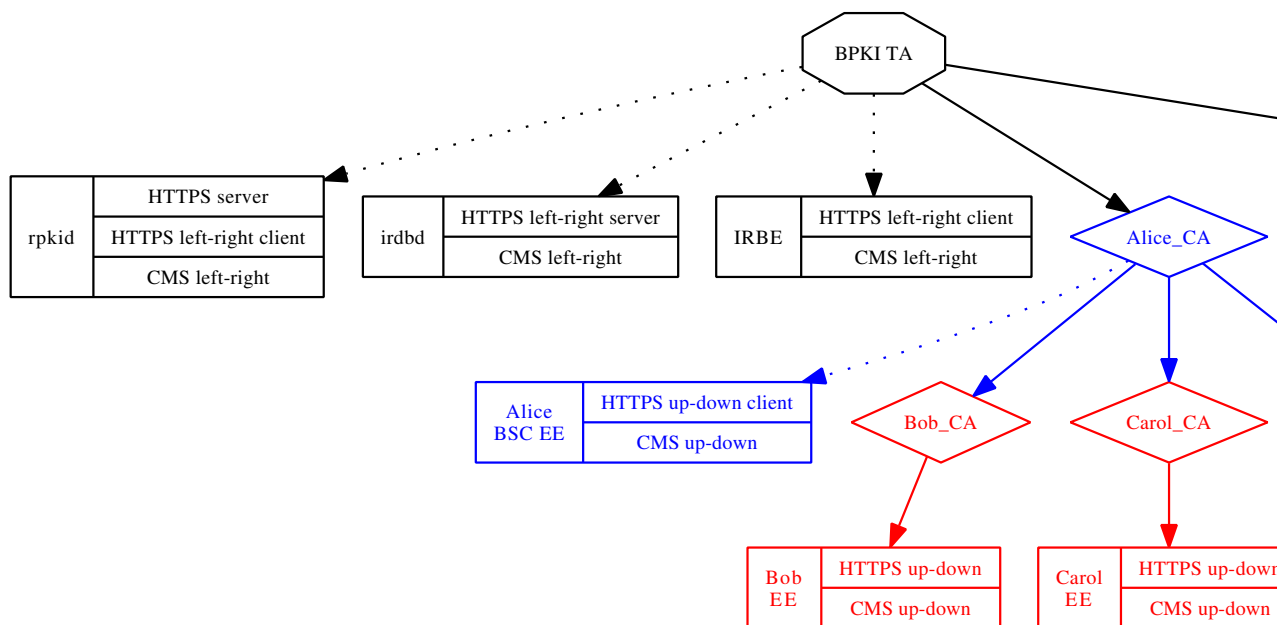
Setup of the BPKI is handled by the back end; for the most part, [rpkid](#) and [pubd](#) just use the result. The one place where the engines are directly involved in creation of new BPKI certificates is in the production of end-entity certificates for use by the engines.

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

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

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

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



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

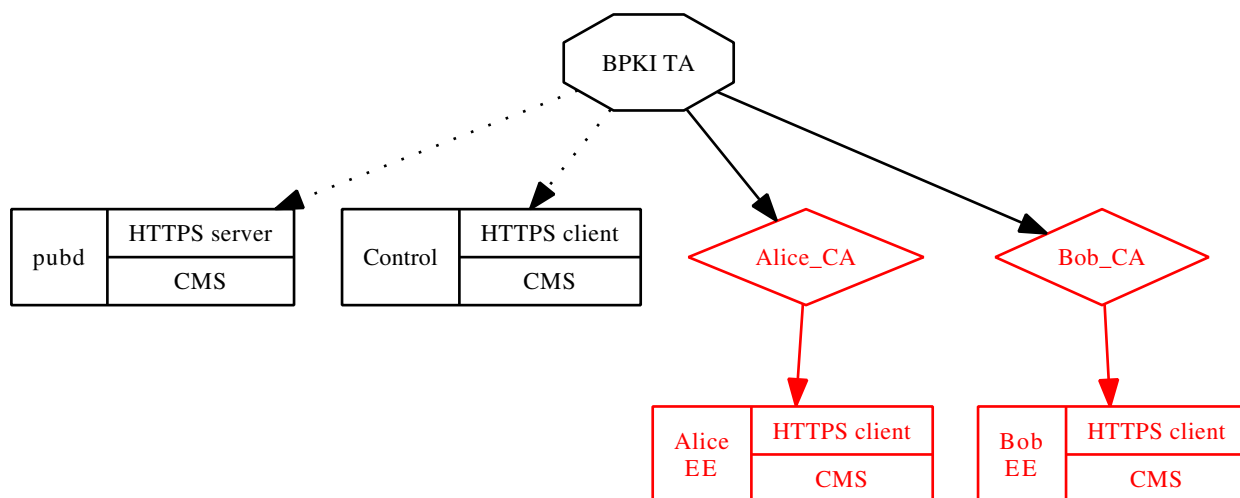
There's one nasty bit where the model had to bend to fit the current state of the underlying protocols: it's not possible to use exactly the same BPKI keys and certificates for HTTPS and CMS. The reason for this is simple: each hosted entity has its own BPKI, as does the hosting entity, but the HTTPS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

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

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

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

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



While it is likely that RIRs (at least) will operate both **rpki** and **pubd** instances, the two functions are conceptually separate. As far as **pubd** is concerned, it doesn't matter who operates the **rpki** instance: **pubd** just has clients, each of which has trust material that has been cross-certified into **pubd**'s BPKI. Similarly, **rpki** 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 **rpki** 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 **rpki** 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 **rpki** and **pubd** require static configuration of the left-right and **publication** control certificates.

9 Namespace Documentation

9.1 Package irbe_cli

Classes

- class [bsc_elt](#)
- class [caller](#)
- 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_sax_handler](#)
- class [list_published_objects_elt](#)
- class [manifest_elt](#)
- class [parent_elt](#)
- class [publication_cms_msg](#)
- class [publication_msg](#)
- class [publication_sax_handler](#)
- class [reply_elt_mixin](#)
- class [report_error_elt](#)
- class [repository_elt](#)
- class [roa_elt](#)
- class [self_elt](#)
- class [UsageWrapper](#)

Functions

- def [usage](#)

Variables

- list [argv](#) = sys.argv[1:]
- tuple [call_pubd](#)
- tuple [call_rpkid](#)
- tuple [cfg](#) = [rpki.config.parser](#)([cfg_file](#), "irbe_cli")
- string [cfg_file](#) = "irbe.conf"

- `pem_out` = None
- `q_msg` = `q_msg_left_right`
- tuple `q_msg_left_right` = `left_right_msg.query()`
- tuple `q_msg_publication` = `publication_msg.query()`
- list `q_pdu` = `left_right_msg.pdus[argv[0]]`
- list `top_opts` = ["config=", "help", "pem_out=", "quiet", "verbose"]
- tuple `usage_fill` = `UsageWrapper(subsequent_indent = " " * 4)`
- `verbose` = True

9.1.1 Detailed Description

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

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

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

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

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

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

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

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

9.1.2 Function Documentation

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

Definition at line 275 of file `irbe_cli.py`.

9.1.3 Variable Documentation

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

Definition at line 294 of file irbe_cli.py.

9.1.3.2 tuple irbe_cli.call_pubd

Initial value:

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

Definition at line 349 of file irbe_cli.py.

9.1.3.3 tuple irbe_cli.call_rpkid

Initial value:

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

Definition at line 337 of file irbe_cli.py.

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

Definition at line 318 of file irbe_cli.py.

9.1.3.5 irbe_cli.cfg_file = "irbe.conf"

Definition at line 299 of file irbe_cli.py.

9.1.3.6 irbe_cli.pem_out = None

Definition at line 39 of file irbe_cli.py.

9.1.3.7 irbe_cli.q_msg = q_msg_left_right

Definition at line 326 of file irbe_cli.py.

9.1.3.8 tuple irbe_cli.q_msg_left_right = left_right_msg.query()

Definition at line 320 of file irbe_cli.py.

9.1.3.9 tuple irbe_cli.q_msg_publication = publication_msg.query()

Definition at line 321 of file irbe_cli.py.

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

Definition at line 325 of file irbe_cli.py.

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

Definition at line 273 of file irbe_cli.py.

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

Definition at line 87 of file irbe_cli.py.

9.1.3.13 irbe_cli.verbose = True

Definition at line 300 of file irbe_cli.py.

9.2 Package irdbd**Functions**

- def [handle_list_resources](#)
- def [handle_list_roa_requests](#)
- def [handler](#)

Variables

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

9.2.1 Detailed Description

IR database daemon.

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

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

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

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

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

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

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

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

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

9.2.2 Function Documentation

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

Definition at line 43 of file irdbd.py.

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

Definition at line 80 of file irdbd.py.

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

Definition at line 109 of file irdbd.py.

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

Definition at line 187 of file irdbd.py.

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

Definition at line 174 of file irdbd.py.

9.2.3.3 irdbd.cfg_file = "irdbd.conf"

Definition at line 162 of file irdbd.py.

9.2.3.4 tuple irdbd.client_ta = (bpki_ta, rpkid_cert)

Definition at line 203 of file irdbd.py.

9.2.3.5 tuple irdbd.cur = db.cursor()

Definition at line 184 of file irdbd.py.

9.2.3.6 tuple irdbd.db

Initial value:

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

Definition at line 180 of file irdbd.py.

9.2.3.7 dictionary irdbd.handle_dispatch

Initial value:

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

Definition at line 105 of file irdbd.py.

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

Definition at line 206 of file irdbd.py.

9.2.3.9 string irdbd.host = "localhost"

Definition at line 204 of file irdbd.py.

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

Definition at line 189 of file irdbd.py.

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

Definition at line 190 of file irdbd.py.

9.2.3.12 int irdbd.port = 443

Definition at line 205 of file irdbd.py.

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

Definition at line 188 of file irdbd.py.

9.2.3.14 irdbd.server_cert = irdbd_cert,

Definition at line 202 of file irdbd.py.

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

Definition at line 176 of file irdbd.py.

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

Definition at line 192 of file irdbd.py.

9.3 Package pubd**Classes**

- class [pubd_context](#)

Functions

- def [main](#)

Variables

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

9.3.1 Detailed Description

RPKI publication engine.

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

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

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

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

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

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

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

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

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

9.3.2 Function Documentation

9.3.2.1 def pubd.main ()

Definition at line 170 of file pubd.py.

9.3.3 Variable Documentation

9.3.3.1 pubd.cfg_file = "pubd.conf"

Definition at line 155 of file pubd.py.

9.3.3.2 pubd.profile = False

Definition at line 156 of file pubd.py.

9.4 Package rootd

Classes

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

Functions

- def [compose_response](#)
- def [del_subject_cert](#)
- def [del_subject_pkcs10](#)
- def [get_root_cert](#)
- def [get_subject_cert](#)
- def [get_subject_pkcs10](#)
- def [issue_subject_cert_maybe](#)
- def [root_newer_than_subject](#)
- def [set_subject_cert](#)
- def [set_subject_pkcs10](#)
- def [up_down_handler](#)

Variables

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

9.4.1 Detailed Description

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

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

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

\$Id: rootd.py 2810 2009-10-03 20:39:38Z sra \$

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

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

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

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

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

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

9.4.2 Function Documentation

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

Definition at line 175 of file rootd.py.

9.4.2.2 `def rootd.del_subject_cert ()`

Definition at line 72 of file rootd.py.

9.4.2.3 `def rootd.del_subject_pkcs10 ()`

Definition at line 91 of file rootd.py.

9.4.2.4 def rootd.get_root_cert ()

Definition at line 48 of file rootd.py.

9.4.2.5 def rootd.get_subject_cert ()

Definition at line 56 of file rootd.py.

9.4.2.6 def rootd.get_subject_pkcs10 ()

Definition at line 77 of file rootd.py.

9.4.2.7 def rootd.issue_subject_cert_maybe (*new_pkcs10*)

Definition at line 98 of file rootd.py.

9.4.2.8 def rootd.root_newer_than_subject ()

Definition at line 53 of file rootd.py.

9.4.2.9 def rootd.set_subject_cert (*cert*)

Definition at line 65 of file rootd.py.

9.4.2.10 def rootd.set_subject_pkcs10 (*pkcs10*)

Definition at line 85 of file rootd.py.

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

Definition at line 238 of file rootd.py.

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

Definition at line 284 of file rootd.py.

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

Definition at line 282 of file rootd.py.

9.4.3.3 rootd.cfg_file = "rootd.conf"

Definition at line 270 of file rootd.py.

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

Definition at line 288 of file rootd.py.

9.4.3.5 tuple rootd.client_ta = (bpki_ta, child_bpki_cert)

Definition at line 312 of file rootd.py.

9.4.3.6 rootd.handlers = up_down_handler)

Definition at line 315 of file rootd.py.

9.4.3.7 `rootd.host = https_server_host,`

Definition at line 313 of file rootd.py.

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

Definition at line 290 of file rootd.py.

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

Definition at line 291 of file rootd.py.

9.4.3.10 `rootd.port = https_server_port,`

Definition at line 314 of file rootd.py.

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

Definition at line 286 of file rootd.py.

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

Definition at line 287 of file rootd.py.

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

Definition at line 285 of file rootd.py.

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

Definition at line 296 of file rootd.py.

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

Definition at line 293 of file rootd.py.

9.4.3.16 `rootd.rpki_root_cert = None`

Definition at line 46 of file rootd.py.

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

Definition at line 299 of file rootd.py.

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

Definition at line 300 of file rootd.py.

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

Definition at line 303 of file rootd.py.

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

Definition at line 295 of file rootd.py.

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

Definition at line 298 of file rootd.py.

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

Definition at line 302 of file rootd.py.

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

Definition at line 304 of file rootd.py.

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

Definition at line 307 of file rootd.py.

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

Definition at line 305 of file rootd.py.

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

Definition at line 308 of file rootd.py.

9.4.3.27 rootd.server_cert = rootd_bpki_cert,

Definition at line 311 of file rootd.py.

9.5 Package rpki

Packages

- package [async](#)
- package [config](#)
- package [exceptions](#)
- package [https](#)
- package [ipaddrs](#)
- package [left_right](#)
- package [log](#)
- package [manifest](#)
- package [oids](#)
- package [publication](#)
- package [relaxng](#)
- package [resource_set](#)
- package [roa](#)
- package [rpki_engine](#)
- package [sql](#)
- package [sundial](#)
- package [up_down](#)
- package [x509](#)
- package [xml_utils](#)

9.6 Package rpki.async

Classes

- class [iterator](#)
- class [sync_wrapper](#)
- class [timer](#)

Functions

- def [_raiseExitNow](#)
- def [event_loop](#)
- def [exit_event_loop](#)

Variables

- `ExitNow` = `asyncore.ExitNow`

9.6.1 Detailed Description

Utilities for event-driven programming.

```
$Id: async.py 2748 2009-09-11 18:03:59Z 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.

9.6.2 Function Documentation

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

Signal handler for `event_loop()`.

Definition at line 218 of file `async.py`.

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

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

Definition at line 222 of file `async.py`.

9.6.2.3 `def rpki.async.exit_event_loop ()`

Force exit from event_loop().

Definition at line 272 of file async.py.

9.6.3 Variable Documentation

9.6.3.1 rpki::async.ExitNow = asyncore.ExitNow

Definition at line 24 of file async.py.

9.7 Package rpki.config

Classes

- class [parser](#)

9.7.1 Detailed Description

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

\$Id: config.py 2637 2009-07-17 23:29:27Z sra \$

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

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

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

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

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

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

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

9.8 Package rpki.exceptions

Classes

- class [BadClassNameSyntax](#)
- class [BadClientURL](#)
- class [BadContactURL](#)
- class [BadExtension](#)
- class [BadIRDBReply](#)
- class [BadIssueResponse](#)
- class [BadPKCS10](#)
- class [BadPublicationReply](#)
- class [BadQuery](#)
- class [BadSender](#)
- class [BadStatusCode](#)
- class [BadURISyntax](#)
- class [BSCNotFound](#)
- class [BSCNotReady](#)
- class [ChildNotFound](#)
- class [ClassNameMismatch](#)
- class [ClassNameUnknown](#)
- class [ClientNotFound](#)
- class [CMSCRLNotSet](#)
- class [CMSVerificationFailed](#)
- class [DBConsistencyError](#)
- class [DERObjectConversionError](#)
- class [DuplicateObject](#)
- class [EmptyPEM](#)
- class [EmptyROAPrefixList](#)
- class [ForbiddenURI](#)
- class [HandleTranslationError](#)
- class [HTTPRequestFailed](#)
- class [HTTPSBadVersion](#)
- class [HTTPSClientAborted](#)
- class [HTTPSUnexpectedState](#)
- class [MissingCMSCRL](#)
- class [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](#)

9.8.1 Detailed Description

Exception definitions for RPKI modules.

```
$Id: exceptions.py 2742 2009-09-09 04:00:31Z sra $
```

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

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

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

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

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

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

9.9 Package rpki.https

Classes

- class [http_client](#)
- class [http_listener](#)
- class [http_message](#)
- class [http_queue](#)
- class [http_request](#)
- class [http_response](#)
- class [http_server](#)
- class [http_stream](#)

Functions

- def [build_https_ta_cache](#)
- def [client](#)
- def [logger](#)
- def [server](#)

Variables

- dictionary [client_queues](#) = { }
- [debug_http](#) = False
- [debug_tls_certs](#) = False
- tuple [default_client_timeout](#) = [rpki.sundial.timedelta](#)(minutes = 15)
- tuple [default_http_version](#) = (1, 0)
- tuple [default_server_timeout](#) = [rpki.sundial.timedelta](#)(minutes = 20)
- string [rpki_content_type](#) = "application/x-rpki"
- [want_persistent_client](#) = True
- [want_persistent_server](#) = True

9.9.1 Detailed Description

HTTPS utilities, both client and server.

At the moment this only knows how to use the PEM certs in my subversion repository; generalizing it would not be hard, but the more general version should use SQL anyway.

\$Id: https.py 2751 2009-09-14 19:27:01Z sra \$

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

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

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

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

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

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

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

9.9.2 Function Documentation

9.9.2.1 `def rpki.https.build_https_ta_cache (certs)`

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

Definition at line 755 of file https.py.

9.9.2.2 `def rpki.https.client (msg, client_key, client_cert, server_ta, url, callback, errback)`

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

Definition at line 696 of file https.py.

9.9.2.3 def rpki.https.logger (self, msg)

Definition at line 173 of file https.py.

9.9.2.4 def rpki.https.server (handlers, server_key, server_cert, port, host = "", client_ta = (), dynamic_https_trust_anchor = None)

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

Definition at line 741 of file https.py.

9.9.3 Variable Documentation**9.9.3.1 dictionary rpki::https.client_queues = {}**

Definition at line 694 of file https.py.

9.9.3.2 rpki::https.debug_http = False

Definition at line 49 of file https.py.

9.9.3.3 rpki::https.debug_tls_certs = False

Definition at line 52 of file https.py.

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

Definition at line 62 of file https.py.

9.9.3.5 tuple rpki::https.default_http_version = (1, 0)

Definition at line 65 of file https.py.

**9.9.3.6 tuple rpki::https.default_server_timeout =
rpki.sundial.timedelta(minutes = 20)**

Definition at line 63 of file https.py.

9.9.3.7 string rpki::https.rpki_content_type = "application/x-rpki"

Definition at line 43 of file https.py.

9.9.3.8 rpki::https.want_persistent_client = True

Definition at line 55 of file https.py.

9.9.3.9 rpki::https.want_persistent_server = True

Definition at line 56 of file https.py.

9.10 Package rpki.ipaddrs**Classes**

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

9.10.1 Detailed Description

Classes to represent IP addresses.

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

the underlying "long" type.

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

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

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

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

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

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

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

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

9.11 Package rpki.left_right

Classes

- class [bsc_elt](#)
- class [child_elt](#)
- class [cms_msg](#)
- class [data_elt](#)
- class [left_right_namespace](#)
- class [list_published_objects_elt](#)
- class [list_resources_elt](#)
- class [list_roa_requests_elt](#)
- class [msg](#)
- class [parent_elt](#)
- class [report_error_elt](#)

- class `repository_elt`
- class `sax_handler`
- class `self_elt`

Variables

- `enforce_strict_up_down_xml_sender = False`

9.11.1 Detailed Description

RPKI "left-right" protocol.

```
$Id: left_right.py 2795 2009-09-29 05:43:17Z sra $
```

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

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

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

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

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

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

9.11.2 Variable Documentation

9.11.2.1 `rpki::left_right.enforce_strict_up_down_xml_sender = False`

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

9.12 Package rpki.log

Classes

- class `logger`

Functions

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

Variables

- tuple `debug` = `logger(syslog.LOG_DEBUG)`
- `enable_trace` = False
Whether call tracing is enabled.
- tuple `error` = `logger(syslog.LOG_ERR)`
- tuple `info` = `logger(syslog.LOG_INFO)`
- tuple `note` = `logger(syslog.LOG_NOTICE)`
- int `pid` = 0
- string `tag` = ""
- `use_syslog` = False
Whether to use syslog.
- tuple `warn` = `logger(syslog.LOG_WARNING)`

9.12.1 Detailed Description

Logging facilities for RPKI libraries.

\$Id: log.py 2732 2009-09-04 19:55:29Z sra \$

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

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

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

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

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

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

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

9.12.2 Function Documentation

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

Initialize logging system.

Definition at line 51 of file log.py.

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

Enable or disable call tracing.

Definition at line 63 of file log.py.

9.12.2.3 `def rpki.log.trace ()`

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

Definition at line 91 of file log.py.

9.12.2.4 def rpki.log.traceback ()

Consolidated backtrace facility with a bit of extra info.

Definition at line 100 of file log.py.

9.12.3 Variable Documentation**9.12.3.1 tuple rpki::log.debug = logger(syslog.LOG_DEBUG)**

Definition at line 89 of file log.py.

9.12.3.2 rpki::log::enable_trace = False

Whether call tracing is enabled.

Definition at line 41 of file log.py.

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

Definition at line 85 of file log.py.

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

Definition at line 88 of file log.py.

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

Definition at line 87 of file log.py.

9.12.3.6 int rpki::log.pid = 0

Definition at line 49 of file log.py.

9.12.3.7 string rpki::log.tag = ""

Definition at line 48 of file log.py.

9.12.3.8 rpki::log::use_syslog = False

Whether to use syslog.

Definition at line 46 of file log.py.

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

Definition at line 86 of file log.py.

9.13 Package rpki.manifest**Classes**

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

9.13.1 Detailed Description

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

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

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

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

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

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

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

9.14 Package rpki.oids

Variables

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

Mapping table of string names to OIDs.

- dictionary `oid2name`

Mapping table of OIDs to conventional string names.

9.14.1 Detailed Description

OID database.

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

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

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

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

9.14.2 Variable Documentation

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

Mapping table of string names to OIDs.

Definition at line 58 of file oids.py.

9.14.2.2 rpki::oids::oid2name

Initial value:

```
{
  (1, 2, 840, 113549, 1, 1, 11) : "sha256WithRSAEncryption",
  (1, 2, 840, 113549, 1, 1, 12) : "sha384WithRSAEncryption",
  (1, 2, 840, 113549, 1, 1, 13) : "sha512WithRSAEncryption",
  (1, 2, 840, 113549, 1, 7, 1) : "id-data",
  (1, 2, 840, 113549, 1, 9, 16) : "id-smime",
  (1, 2, 840, 113549, 1, 9, 16, 1) : "id-ct",
  (1, 2, 840, 113549, 1, 9, 16, 1, 24) : "id-ct-routeOriginAttestation",
  (1, 2, 840, 113549, 1, 9, 16, 1, 26) : "id-ct-rpkiManifest",
  (1, 2, 840, 113549, 1, 9, 16, 1, 28) : "id-ct-xml",
  (1, 3, 6, 1, 5, 5, 7, 1, 1) : "authorityInfoAccess",
  (1, 3, 6, 1, 5, 5, 7, 1, 11) : "subjectInfoAccess",
  (1, 3, 6, 1, 5, 5, 7, 1, 7) : "sbgp-ipAddrBlock",
  (1, 3, 6, 1, 5, 5, 7, 1, 8) : "sbgp-autonomousSysNum",
  (1, 3, 6, 1, 5, 5, 7, 14, 2) : "id-cp-ipAddr-asNumber",
  (1, 3, 6, 1, 5, 5, 7, 48, 2) : "id-ad-caIssuers",
  (1, 3, 6, 1, 5, 5, 7, 48, 5) : "id-ad-caRepository",
  (1, 3, 6, 1, 5, 5, 7, 48, 9) : "id-ad-signedObjectRepository",
  (1, 3, 6, 1, 5, 5, 7, 48, 10) : "id-ad-rpkiManifest",
  (1, 3, 6, 1, 5, 5, 7, 48, 11) : "id-ad-signedObject",
  (2, 16, 840, 1, 101, 3, 4, 2, 1) : "id-sha256",
  (2, 5, 29, 14) : "subjectKeyIdentifier",
  (2, 5, 29, 15) : "keyUsage",
  (2, 5, 29, 19) : "basicConstraints",
  (2, 5, 29, 20) : "cRLNumber",
  (2, 5, 29, 31) : "cRLDistributionPoints",
  (2, 5, 29, 32) : "certificatePolicies",
  (2, 5, 29, 35) : "authorityKeyIdentifier",
  (2, 5, 4, 3) : "commonName",
}
```

Mapping table of OIDs to conventional string names.

Definition at line 24 of file oids.py.

9.15 Package rpki.publication

Classes

- class [certificate_elt](#)
- class [client_elt](#)
- class [cms_msg](#)
- class [config_elt](#)

- class [control_elt](#)
- class [crl_elt](#)
- class [manifest_elt](#)
- class [msg](#)
- class [publication_namespace](#)
- class [publication_object_elt](#)
- class [report_error_elt](#)
- class [roa_elt](#)
- class [sax_handler](#)

9.15.1 Detailed Description

RPKI "publication" protocol.

\$Id: publication.py 2798 2009-09-30 02:25:05Z sra \$

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

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

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

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

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

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

9.16 Package rpki.relaxng

Variables

- tuple [left_right](#)
Parsed RelaxNG [left_right](#) schema.

- tuple [publication](#)
Parsed RelaxNG [publication](#) schema.
- tuple [up_down](#)
Parsed RelaxNG [up_down](#) schema.

9.16.1 Variable Documentation

9.16.1.1 rpki::relaxng::left_right

Parsed RelaxNG [left_right](#) schema.

Definition at line 7 of file relaxng.py.

9.16.1.2 rpki::relaxng::publication

Parsed RelaxNG [publication](#) schema.

Definition at line 1171 of file relaxng.py.

9.16.1.3 rpki::relaxng::up_down

Parsed RelaxNG [up_down](#) schema.

Definition at line 917 of file relaxng.py.

9.17 Package rpki.resource_set

Classes

- class [resource_bag](#)
- class [resource_range](#)
- class [resource_range_as](#)
- class [resource_range_ip](#)
- class [resource_range_ipv4](#)
- class [resource_range_ipv6](#)
- class [resource_set](#)

- class `resource_set_as`
- class `resource_set_ip`
- class `resource_set_ipv4`
- class `resource_set_ipv6`
- class `roa_prefix`
- class `roa_prefix_ipv4`
- class `roa_prefix_ipv6`
- class `roa_prefix_set`
- class `roa_prefix_set_ipv4`
- class `roa_prefix_set_ipv6`

Functions

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

Variables

- string `inherit_token` = "<inherit>"

Token used to indicate inheritance in read and print syntax.

9.17.1 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 2776 2009-09-19 03:26:51Z sra \$

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

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

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT,

INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

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

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

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

9.17.2 Function Documentation

9.17.2.1 `def rpki.resource_set._bs2long (bs, addrlen, fill) [private]`

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

Definition at line 514 of file `resource_set.py`.

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

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

Definition at line 526 of file `resource_set.py`.

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

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

Definition at line 190 of file `resource_set.py`.

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

Definition at line 884 of file resource_set.py.

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

Definition at line 917 of file resource_set.py.

9.17.3 Variable Documentation**9.17.3.1 rpki::resource_set::inherit_token = "<inherit>"**

Token used to indicate inheritance in read and print syntax.

Definition at line 48 of file resource_set.py.

9.18 Package rpki.roa**Classes**

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

9.18.1 Detailed Description

ROA (Route Origin Authorization).

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

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

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

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

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above

copyright notice and this permission notice appear in all copies.

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

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

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

ASID ::= INTEGER

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

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

IPAddress ::= BIT STRING
```

9.19 Package rpki.rpki_engine

Classes

- class [ca_detail_obj](#)
- class [ca_obj](#)
- class [child_cert_obj](#)
- class [revoked_cert_obj](#)
- class [roa_obj](#)
- class [rpkid_context](#)

9.19.1 Detailed Description

Global context for rpkid.

\$Id: rpki_engine.py 2793 2009-09-29 05:26:38Z sra \$

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

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

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

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

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

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

9.20 Package rpki.sql

Classes

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

9.20.1 Detailed Description

SQL interface code.

\$Id: sql.py 2648 2009-07-20 18:49:10Z sra \$

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

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

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

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

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

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

9.21 Package rpki.sundial

Classes

- class `datetime`
- class `timedelta`

Functions

- def `_cast`
- def `now`
- def `test`

9.21.1 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 2785 2009-09-25 20:21:53Z sra $
```

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

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

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH

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

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

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

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

9.21.2 Function Documentation

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

Cast result of arithmetic operations back into correct subtype.

Definition at line 232 of file sundial.py.

9.21.2.2 `def rpki.sundial.now ()`

Get current timestamp.

Definition at line 50 of file sundial.py.

9.21.2.3 `def rpki.sundial.test (t)`

Definition at line 244 of file sundial.py.

9.22 Package rpki.up_down

Classes

- class [base_elt](#)
- class [certificate_elt](#)
- class [class_elt](#)
- class [class_response_syntax](#)
- class [cms_msg](#)
- class [error_response_pdu](#)
- class [issue_pdu](#)
- class [issue_response_pdu](#)
- class [list_pdu](#)
- class [list_response_pdu](#)
- class [message_pdu](#)
- class [multi_uri](#)
- class [revoke_pdu](#)
- class [revoke_response_pdu](#)
- class [revoke_syntax](#)
- class [sax_handler](#)

Variables

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

9.22.1 Detailed Description

RPKI "up-down" protocol.

```
$Id: up_down.py 2793 2009-09-29 05:26:38Z sra $
```

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

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

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

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

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

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

9.22.2 Variable Documentation

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

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

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

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

9.23 Package rpki.x509

Classes

- class [CMS_object](#)
- class [CRL](#)
- class [DER_CMS_object](#)
- class [DER_object](#)
- class [PEM_converter](#)
- class [PKCS10](#)
- class [ROA](#)
- class [RSA](#)
- class [RSAPublic](#)
- class [SignedManifest](#)
- class [X509](#)
- class [XML_CMS_object](#)

Functions

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

9.23.1 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 2784 2009-09-25 19:13:06Z sra \$

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

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

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

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

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

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

9.23.2 Function Documentation

9.23.2.1 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 50 of file x509.py.

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

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

Definition at line 691 of file x509.py.

9.24 Package rpki.xml_utils

Classes

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

9.24.1 Detailed Description

XML utilities.

\$Id: xml_utils.py 2791 2009-09-29 00:06:00Z sra \$

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

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

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM

LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

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

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

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

9.25 Package rpkiid

Functions

- def `main`

Variables

- string `cfg_file` = "rpkiid.conf"
- `profile` = None

9.25.1 Detailed Description

RPKI engine daemon. This is still very much a work in progress.

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

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

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

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

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

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM

LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

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

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

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

9.25.2 Function Documentation

9.25.2.1 `def rpkid.main ()`

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

9.25.3 Variable Documentation

9.25.3.1 `rpkid.cfg_file = "rpkid.conf"`

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

9.25.3.2 `rpkid.profile = None`

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

10 Class Documentation

10.1 `async_chat` Class Reference

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

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

- [https.py \(2751\)](#)

10.2 dispatcher Class Reference

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

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

- [https.py \(2751\)](#)

10.3 Exception Class Reference

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

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

- [exceptions.py \(2742\)](#)

10.4 irbe_cli.bsc_elt Class Reference

Inherits [irbe_cli::cmd_elt_mixin](#), and [rpki::left_right::bsc_elt](#).

Public Member Functions

- def [client_query_signing_cert](#)
- def [client_query_signing_cert_crl](#)
- def [client_reply_decode](#)

Public Attributes

- [signing_cert](#)
- [signing_cert_crl](#)

Static Public Attributes

- tuple [excludes](#) = ("pkcs10_request",)
XML attributes and elements that should not be allowed as command line arguments.

10.4.1 Detailed Description

Definition at line 189 of file [irbe_cli.py](#).

10.4.2 Member Function Documentation

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

--signing_cert option.

Definition at line 193 of file irbe_cli.py.

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

--signing_cert_crl option.

Definition at line 197 of file irbe_cli.py.

10.4.2.3 def irbe_cli.bsc_elt.client_reply_decode (self)

Reimplemented from [irbe_cli.reply_elt_mixin](#).

Definition at line 201 of file irbe_cli.py.

10.4.3 Member Data Documentation

10.4.3.1 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 191 of file irbe_cli.py.

10.4.3.2 irbe_cli.bsc_elt.signing_cert

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

Definition at line 195 of file irbe_cli.py.

10.4.3.3 irbe_cli.bsc_elt.signing_cert_crl

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

Definition at line 199 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2799\)](#)

10.5 irbe_cli.caller Class Reference

Inherits [object](#).

Public Member Functions

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

Public Attributes

- [client_cert](#)
- [client_key](#)
- [cms_class](#)
- [server_cert](#)
- [server_ta](#)
- [url](#)

10.5.1 Detailed Description

Handle client-side mechanics for left-right and publication protocols.

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

10.5.2 Member Function Documentation

10.5.2.1 `def irbe_cli.caller.__call__(self, cb, eb, msg)`

Definition at line 55 of file `irbe_cli.py`.

10.5.2.2 `def irbe_cli.caller.__init__ (self, cms_class, client_key, client_cert, server_ta, server_cert, url)`

Definition at line 47 of file irbe_cli.py.

10.5.3 Member Data Documentation

10.5.3.1 irbe_cli.caller.client_cert

Definition at line 50 of file irbe_cli.py.

10.5.3.2 irbe_cli.caller.client_key

Definition at line 49 of file irbe_cli.py.

10.5.3.3 irbe_cli.caller.cms_class

Definition at line 48 of file irbe_cli.py.

10.5.3.4 irbe_cli.caller.server_cert

Definition at line 52 of file irbe_cli.py.

10.5.3.5 irbe_cli.caller.server_ta

Definition at line 51 of file irbe_cli.py.

10.5.3.6 irbe_cli.caller.url

Definition at line 53 of file irbe_cli.py.

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

- [irbe_cli.py \(2799\)](#)

10.6 `irbe_cli.certificate_elt` Class Reference

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

10.6.1 Detailed Description

Definition at line 246 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2799\)](#)

10.7 `irbe_cli.child_elt` Class Reference

Inherits [irbe_cli::cmd_elt_mixin](#), and [rpki::left_right::child_elt](#).

10.7.1 Detailed Description

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

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

- [irbe_cli.py \(2799\)](#)

10.8 `irbe_cli.client_elt` Class Reference

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

10.8.1 Detailed Description

Definition at line 243 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2799\)](#)

10.9 `irbe_cli.cmd_elt_mixin` Class Reference

Inherits [irbe_cli::reply_elt_mixin](#).

Inherited by [irbe_cli.bsc_elt](#), [irbe_cli.certificate_elt](#), [irbe_cli.child_elt](#), [irbe_cli.client_elt](#), [irbe_cli.config_elt](#), [irbe_cli.crl_elt](#), [irbe_cli.list_published_objects_elt](#), [irbe_cli.manifest_elt](#), [irbe_cli.parent_elt](#), [irbe_cli.repository_elt](#), [irbe_cli.roa_elt](#), and [irbe_cli.self_elt](#).

Public Member Functions

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

Public Attributes

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

Static Public Attributes

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

10.9.1 Detailed Description

Protocol mix-in for command line client element PDUs.

Definition at line 105 of file [irbe_cli.py](#).

10.9.2 Member Function Documentation

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

Parse options for this class.

Definition at line 129 of file irbe_cli.py.

10.9.2.2 def irbe_cli.cmd_elt_mixin.client_query_bpki_cert (*self*, *arg*)

Special handler for --bpki_cert option.

Definition at line 146 of file irbe_cli.py.

10.9.2.3 def irbe_cli.cmd_elt_mixin.client_query_bpki_cms_cert (*self*, *arg*)

Special handler for --bpki_cms_cert option.

Definition at line 154 of file irbe_cli.py.

10.9.2.4 def irbe_cli.cmd_elt_mixin.client_query_bpki_https_cert (*self*, *arg*)

Special handler for --bpki_https_cert option.

Definition at line 162 of file irbe_cli.py.

10.9.2.5 def irbe_cli.cmd_elt_mixin.client_query_cms_glue (*self*, *arg*)

Special handler for --bpki_cms_glue option.

Definition at line 158 of file irbe_cli.py.

10.9.2.6 def irbe_cli.cmd_elt_mixin.client_query_glue (*self*, *arg*)

Special handler for --bpki_glue option.

Definition at line 150 of file irbe_cli.py.

10.9.2.7 def irbe_cli.cmd_elt_mixin.client_query_https_glue (*self*, *arg*)

Special handler for --bpki_https_glue option.

Definition at line 166 of file irbe_cli.py.

10.9.2.8 def irbe_cli.cmd_elt_mixin.usage (*cls*)

Generate usage message for this PDU.

Definition at line 118 of file irbe_cli.py.

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

Definition at line 148 of file irbe_cli.py.

10.9.3.2 irbe_cli.cmd_elt_mixin.bpki_cms_cert

Definition at line 156 of file irbe_cli.py.

10.9.3.3 irbe_cli.cmd_elt_mixin.bpki_cms_glue

Definition at line 160 of file irbe_cli.py.

10.9.3.4 `irbe_cli.cmd_elt_mixin.bpk_i_glue`

Definition at line 152 of file `irbe_cli.py`.

10.9.3.5 `irbe_cli.cmd_elt_mixin.bpk_i_https_cert`

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

10.9.3.6 `irbe_cli.cmd_elt_mixin.bpk_i_https_glue`

Definition at line 168 of file `irbe_cli.py`.

10.9.3.7 `irbe_cli.cmd_elt_mixin::excludes = ()` `[static]`

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

Reimplemented in [irbe_cli.bsc_elt](#), and [irbe_cli.list_published_objects_elt](#).

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

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

Reimplemented from [irbe_cli.reply_elt_mixin](#).

Definition at line 110 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2799\)](#)

10.10 `irbe_cli.cmd_msg_mixin` Class Reference

Inherits [object](#).

Inherited by [irbe_cli.left_right_msg](#), and [irbe_cli.publication_msg](#).

Public Member Functions

- def [usage](#)

10.10.1 Detailed Description

Protocol mix-in for command line client message PDUs.

Definition at line 170 of file `irbe_cli.py`.

10.10.2 Member Function Documentation

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

Generate usage message for this PDU.

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

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

- [irbe_cli.py \(2799\)](#)

10.11 `irbe_cli.config_elt` Class Reference

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

Public Member Functions

- def [client_query_bpki_crl](#)

Public Attributes

- [bpki_crl](#)

10.11.1 Detailed Description

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

10.11.2 Member Function Documentation

10.11.2.1 `def irbe_cli.config_elt.client_query_bpki_crl (self, arg)`

Special handler for `--bpki_crl` option.

Definition at line 239 of file `irbe_cli.py`.

10.11.3 Member Data Documentation

10.11.3.1 `irbe_cli.config_elt.bpki_crl`

Definition at line 241 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2799\)](#)

10.12 irbe_cli.crl_elt Class Reference

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

10.12.1 Detailed Description

Definition at line 249 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2799\)](#)

10.13 irbe_cli.left_right_cms_msg Class Reference

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

Static Public Attributes

- [saxify](#) = `left_right_sax_handler.saxify`

10.13.1 Detailed Description

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

10.13.2 Member Data Documentation

10.13.2.1 `irbe_cli.left_right_cms_msg.saxify = left_right_sax_handler.saxify` [static]

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

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

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

- [irbe_cli.py \(2799\)](#)

10.14 `irbe_cli.left_right_msg` Class Reference

Inherits [irbe_cli::cmd_msg_mixin](#), and [rpki::left_right::msg](#).

Static Public Attributes

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

10.14.1 Detailed Description

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

10.14.2 Member Data Documentation

10.14.2.1 tuple `irbe_cli.left_right_msg.pdus` [static]

Initial value:

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

Dispatch table of PDUs for this protocol.

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

Definition at line 225 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2799\)](#)

10.15 `irbe_cli.left_right_sax_handler` Class Reference

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

Static Public Attributes

- `pdu = left_right_msg`

10.15.1 Detailed Description

Definition at line 229 of file `irbe_cli.py`.

10.15.2 Member Data Documentation

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

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

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

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

- [irbe_cli.py \(2799\)](#)

10.16 `irbe_cli.list_published_objects_elt` Class Reference

Inherits [irbe_cli::cmd_elt_mixin](#), and [rpki::left_right::list_published_objects_elt](#).

Static Public Attributes

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

10.16.1 Detailed Description

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

10.16.2 Member Data Documentation

10.16.2.1 `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 219 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2799\)](#)

10.17 `irbe_cli.manifest_elt` Class Reference

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

10.17.1 Detailed Description

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

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

- [irbe_cli.py \(2799\)](#)

10.18 `irbe_cli.parent_elt` Class Reference

Inherits [irbe_cli::cmd_elt_mixin](#), and [rpki::left_right::parent_elt](#).

10.18.1 Detailed Description

Definition at line 208 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2799\)](#)

10.19 `irbe_cli.publication_cms_msg` Class Reference

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

Static Public Attributes

- [saxify](#) = `publication_sax_handler.saxify`

10.19.1 Detailed Description

Definition at line 268 of file `irbe_cli.py`.

10.19.2 Member Data Documentation

10.19.2.1 `irbe_cli.publication_cms_msg.saxify = publication_sax_handler.saxify` [static]

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

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

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

- [irbe_cli.py \(2799\)](#)

10.20 `irbe_cli.publication_msg` Class Reference

Inherits [irbe_cli::cmd_msg_mixin](#), and [rpki::publication::msg](#).

Static Public Attributes

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

10.20.1 Detailed Description

Definition at line 261 of file `irbe_cli.py`.

10.20.2 Member Data Documentation

10.20.2.1 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 262 of file irbe_cli.py.

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

- [irbe_cli.py \(2799\)](#)

10.21 irbe_cli.publication_sax_handler Class Reference

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

Static Public Attributes

- [pdu = publication_msg](#)

10.21.1 Detailed Description

Definition at line 265 of file irbe_cli.py.

10.21.2 Member Data Documentation

10.21.2.1 irbe_cli.publication_sax_handler.pdu = publication_msg [static]

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

Definition at line 266 of file irbe_cli.py.

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

- [irbe_cli.py \(2799\)](#)

10.22 irbe_cli.reply_elt_mixin Class Reference

Inherits [object](#).

Inherited by [irbe_cli.cmd_elt_mixin](#), [irbe_cli.report_error_elt](#), and [irbe_cli.report_error_elt](#).

Public Member Functions

- def [client_reply_decode](#)
- def [client_reply_show](#)

Static Public Attributes

- [is_cmd](#) = False

10.22.1 Detailed Description

Protocol mix-in for printout of reply PDUs.

Definition at line 89 of file [irbe_cli.py](#).

10.22.2 Member Function Documentation

10.22.2.1 def [irbe_cli.reply_elt_mixin.client_reply_decode](#) (*self*)

Reimplemented in [irbe_cli.bsc_elt](#).

Definition at line 96 of file [irbe_cli.py](#).

10.22.2.2 def [irbe_cli.reply_elt_mixin.client_reply_show](#) (*self*)

Definition at line 99 of file [irbe_cli.py](#).

10.22.3 Member Data Documentation

10.22.3.1 [irbe_cli.reply_elt_mixin.is_cmd](#) = False [static]

Reimplemented in [irbe_cli.cmd_elt_mixin](#).

Definition at line 94 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2799\)](#)

10.23 `irbe_cli.report_error_elt` Class Reference

Inherits [irbe_cli::reply_elt_mixin](#), [rpki::publication::report_error_elt](#), [irbe_cli::reply_elt_mixin](#), and [rpki::left_right::report_error_elt](#).

10.23.1 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 \(2799\)](#)

10.24 `irbe_cli.repository_elt` Class Reference

Inherits [irbe_cli::cmd_elt_mixin](#), and [rpki::left_right::repository_elt](#).

10.24.1 Detailed Description

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

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

- [irbe_cli.py \(2799\)](#)

10.25 `irbe_cli.roa_elt` Class Reference

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

10.25.1 Detailed Description

Definition at line 255 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2799\)](#)

10.26 `irbe_cli.self_elt` Class Reference

Inherits [irbe_cli::cmd_elt_mixin](#), and [rpki::left_right::self_elt](#).

10.26.1 Detailed Description

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

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

- [irbe_cli.py \(2799\)](#)

10.27 `irbe_cli.UsageWrapper` Class Reference

Inherits [textwrap::TextWrapper](#).

Public Member Functions

- `def __call__`

10.27.1 Detailed Description

Call interface around Python `textwrap.TextWrapper` class.

Definition at line 78 of file `irbe_cli.py`.

10.27.2 Member Function Documentation

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

Format arguments, with `TextWrapper` indentation.

Definition at line 83 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2799\)](#)

10.28 long Class Reference

Inherited by [rpki.ipaddrs.v4addr](#), and [rpki.ipaddrs.v6addr](#).

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

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

10.29 object Class Reference

Inherited by [irbe_cli.caller](#), [irbe_cli.cmd_msg_mixin](#), [irbe_cli.reply_elt_mixin](#), [pubd.pubd_context](#), [rpki.async.iterator](#), [rpki.async.sync_wrapper](#), [rpki.async.timer](#), [rpki.config.parser](#), [rpki.https.http_message](#), [rpki.https.http_queue](#), [rpki.left_right.left_right_namespace](#), [rpki.log.logger](#), [rpki.publication.publication_namespace](#), [rpki.resource_set.resource_bag](#), [rpki.resource_set.resource_range](#), [rpki.resource_set.roa_prefix](#), [rpki.rpki_engine.rpkid_context](#), [rpki.sql.session](#), [rpki.sql.sql_persistent](#), [rpki.sql.template](#), [rpki.up_down.base_elt](#), [rpki.x509.DER_object](#), [rpki.x509.PEM_converter](#), and [rpki.xml_utils.base_elt](#).

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

- [x509.py \(2784\)](#)

10.30 pubd.pubd_context Class Reference

Inherits [object](#).

Public Member Functions

- def [__init__](#)
- def [build_https_ta_cache](#)
- def [clear_https_ta_cache](#)
- def [client_handler](#)
- def [control_handler](#)
- def [handler_common](#)

Public Attributes

- [bpki_ta](#)
- [https_server_host](#)
- [https_server_port](#)
- [irbe_cert](#)
- [pubd_cert](#)

- [pubd_key](#)
- [publication_base](#)
- [sql](#)

Static Public Attributes

- tuple [client_url_regexp](#) = re.compile("/client/([-A-Z0-9_]+)\$", re.I)
- [https_ta_cache](#) = None
HTTPS trust anchor cache, to avoid regenerating it for every TLS connection.

10.30.1 Detailed Description

A container for various pubd parameters.

Definition at line 46 of file pubd.py.

10.30.2 Member Function Documentation

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

Definition at line 51 of file pubd.py.

10.30.2.2 def pubd.pubd_context.build_https_ta_cache (self)

Build dynamic TLS trust anchors.

Definition at line 138 of file pubd.py.

10.30.2.3 def pubd.pubd_context.clear_https_ta_cache (self)

Clear dynamic TLS trust anchors.

Definition at line 130 of file pubd.py.

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

Process one PDU from a client.

Definition at line 98 of file pubd.py.

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

Process one PDU from the IRBE.

Definition at line 78 of file pubd.py.

**10.30.2.6 def pubd.pubd_context.handler_common (*self*, *query*, *client*, *cb*,
certs, *crl* = None)**

Common PDU handler code.

Definition at line 65 of file pubd.py.

10.30.3 Member Data Documentation**10.30.3.1 pubd.pubd_context.bpki_ta**

Definition at line 55 of file pubd.py.

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

Definition at line 96 of file pubd.py.

10.30.3.3 pubd.pubd_context.https_server_host

Definition at line 60 of file pubd.py.

10.30.3.4 pubd.pubd_context.https_server_port

Definition at line 61 of file pubd.py.

10.30.3.5 pubd.pubd_context::https_ta_cache = None [static]

HTTPS trust anchor cache, to avoid regenerating it for every TLS connection.

Definition at line 128 of file pubd.py.

10.30.3.6 pubd.pubd_context.irbe_cert

Definition at line 56 of file pubd.py.

10.30.3.7 pubd.pubd_context.pubd_cert

Definition at line 57 of file pubd.py.

10.30.3.8 pubd.pubd_context.pubd_key

Definition at line 58 of file pubd.py.

10.30.3.9 pubd.pubd_context.publication_base

Definition at line 63 of file pubd.py.

10.30.3.10 pubd.pubd_context.sql

Definition at line 53 of file pubd.py.

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

- [pubd.py \(2799\)](#)

10.31 **datetime Class Reference**

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

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

- [sundial.py \(2785\)](#)

10.32 **timedelta Class Reference**

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

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

- [sundial.py \(2785\)](#)

10.33 **rootd.cms_msg Class Reference**

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

Static Public Attributes

- [saxify](#) = sax_handler.saxify

10.33.1 Detailed Description

Definition at line 235 of file rootd.py.

10.33.2 Member Data Documentation

10.33.2.1 **rootd.cms_msg.saxify = sax_handler.saxify** [static]

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

Definition at line 236 of file rootd.py.

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

- [rootd.py \(2810\)](#)

10.34 rootd.issue_pdu Class Reference

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

Public Member Functions

- def [serve_pdu](#)

10.34.1 Detailed Description

Definition at line 194 of file rootd.py.

10.34.2 Member Function Documentation

10.34.2.1 def rootd.issue_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *callback*, *errback*)

Serve one issue request PDU.

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

Definition at line 195 of file rootd.py.

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

- [rootd.py](#) (2810)

10.35 rootd.list_pdu Class Reference

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

Public Member Functions

- def [serve_pdu](#)

10.35.1 Detailed Description

Definition at line 188 of file rootd.py.

10.35.2 Member Function Documentation

10.35.2.1 `def rootd.list_pdu.serve_pdu (self, q_msg, r_msg, child, callback, errback)`

Serve one "list" PDU.

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

Definition at line 189 of file rootd.py.

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

- [rootd.py \(2810\)](#)

10.36 rootd.message_pdu Class Reference

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

Public Member Functions

- `def log_query`

Static Public Attributes

- dictionary [name2type](#)
- tuple [type2name](#) = dict((v, k) for k, v in name2type.items())

10.36.1 Detailed Description

Definition at line 213 of file rootd.py.

10.36.2 Member Function Documentation

10.36.2.1 `def rootd.message_pdu.log_query (self, child)`

Log query we're handling.

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

Definition at line 226 of file rootd.py.

10.36.3 Member Data Documentation

10.36.3.1 dictionary rootd.message_pdu.name2type [static]

Initial value:

```
{
    "list"           : list_pdu,
    "list_response"  : rpki.up_down.list_response_pdu,
    "issue"          : issue_pdu,
    "issue_response" : rpki.up_down.issue_response_pdu,
    "revoke"         : revoke_pdu,
    "revoke_response": rpki.up_down.revoke_response_pdu,
    "error_response" : rpki.up_down.error_response_pdu }
```

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

Definition at line 215 of file rootd.py.

10.36.3.2 tuple rootd.message_pdu.type2name = dict((v, k) for k, v in name2type.items()) [static]

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

Definition at line 224 of file rootd.py.

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

- [rootd.py \(2810\)](#)

10.37 rootd.revoke_pdu Class Reference

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

Public Member Functions

- def [serve_pdu](#)

10.37.1 Detailed Description

Definition at line 201 of file rootd.py.

10.37.2 Member Function Documentation

10.37.2.1 `def rootd.revoke_pdu.serve_pdu (self, q_msg, r_msg, child, cb, eb)`

Serve one revoke request PDU.

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

Definition at line 202 of file rootd.py.

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

- [rootd.py \(2810\)](#)

10.38 rootd.sax_handler Class Reference

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

Static Public Attributes

- `pdu` = [message_pdu](#)

10.38.1 Detailed Description

Definition at line 232 of file rootd.py.

10.38.2 Member Data Documentation

10.38.2.1 `rootd.sax_handler.pdu = message_pdu` [static]

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

Definition at line 233 of file rootd.py.

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

- [rootd.py \(2810\)](#)

10.39 rpki.async.iterator Class Reference

Inherits [object](#).

Public Member Functions

- [def __call__](#)
- [def __init__](#)
- [def __repr__](#)
- [def doit](#)
- [def ignore](#)

Public Attributes

- [caller_function](#)
- [done_callback](#)
- [item_callback](#)
- [iterator](#)
- [timer](#)

10.39.1 Detailed Description

Iteration construct for event-driven code. Takes three arguments:

- Some kind of iterable object
- A callback to call on each item in the iteration
- A callback to call after the iteration terminates.

The item callback receives two arguments: the callable iterator object and the current value of the iteration. It should call the iterator (or arrange for the iterator to be called) when it is time to continue to the next item in the iteration.

The termination callback receives no arguments.

Definition at line 26 of file `async.py`.

10.39.2 Member Function Documentation

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

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

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

Definition at line 45 of file async.py.

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

Definition at line 59 of file async.py.

10.39.2.4 `def rpki.async.iterator.doit (self)`

Definition at line 70 of file async.py.

10.39.2.5 `def rpki.async.iterator.ignore (self, ignored)`

Definition at line 77 of file async.py.

10.39.3 Member Data Documentation

10.39.3.1 `rpki.async.iterator.caller_function`

Definition at line 48 of file async.py.

10.39.3.2 `rpki.async.iterator.done_callback`

Definition at line 47 of file async.py.

10.39.3.3 `rpki.async.iterator.item_callback`

Definition at line 46 of file async.py.

10.39.3.4 rpki.async.iterator.iterator

Definition at line 51 of file async.py.

10.39.3.5 rpki.async.iterator.timer

Definition at line 49 of file async.py.

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

- [async.py \(2748\)](#)

10.40 rpki.async.sync_wrapper Class Reference

Inherits [object](#).

Public Member Functions

- [def __call__](#)
- [def __init__](#)
- [def cb](#)
- [def eb](#)

Public Attributes

- [func](#)

Static Public Attributes

- [err](#) = None
- [res](#) = None

10.40.1 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 239 of file async.py.

10.40.2 Member Function Documentation

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

Definition at line 265 of file async.py.

10.40.2.2 `def rpki.async.sync_wrapper.__init__ (self, func)`

Definition at line 254 of file async.py.

10.40.2.3 `def rpki.async.sync_wrapper.cb (self, res = None)`

Definition at line 257 of file async.py.

10.40.2.4 `def rpki.async.sync_wrapper.eb (self, err)`

Definition at line 261 of file async.py.

10.40.3 Member Data Documentation

10.40.3.1 `rpki.async.sync_wrapper.err = None` `[static]`

Definition at line 252 of file async.py.

10.40.3.2 `rpki.async.sync_wrapper.func`

Definition at line 255 of file async.py.

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

Definition at line 251 of file `async.py`.

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

- [async.py \(2748\)](#)

10.41 rpki.async.timer Class Reference

Inherits [object](#).

Public Member Functions

- def [__cmp__](#)
- 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](#)

Public Attributes

- [errback](#)
- [handler](#)
- [when](#)

Static Public Attributes

- list [queue](#) = []
Timer queue, shared by all [timer](#) instances (there can be only one queue).

10.41.1 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 80 of file `async.py`.

10.41.2 Member Function Documentation

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

Definition at line 124 of file `async.py`.

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

Definition at line 100 of file `async.py`.

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

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

10.41.2.4 `def rpki.async.timer.cancel (self)`

Cancel a timer, if it was set.

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

10.41.2.5 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 209 of file `async.py`.

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

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

Definition at line 157 of file `async.py`.

10.41.2.7 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 140 of file `async.py`.

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

Test whether this timer is currently set.

Definition at line 136 of file `async.py`.

10.41.2.9 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 169 of file `async.py`.

10.41.2.10 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 187 of file async.py.

10.41.2.11 def rpki.async.timer.set (*self*, *when*)

Set a timer. Argument can be a datetime, to specify an absolute time, a timedelta, to specify an offset time, or None, to indicate that the timer should expire immediately, which can be useful in avoiding an excessively deep call stack.

Definition at line 106 of file async.py.

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

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

Definition at line 164 of file async.py.

10.41.2.13 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 147 of file async.py.

10.41.3 Member Data Documentation

10.41.3.1 `rpki.async.timer.errback`

Definition at line 166 of file `async.py`.

10.41.3.2 `rpki.async.timer.handler`

Definition at line 155 of file `async.py`.

10.41.3.3 `rpki::async.timer::queue = []` `[static]`

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

Definition at line 98 of file `async.py`.

10.41.3.4 `rpki.async.timer.when`

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

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

- [async.py \(2748\)](#)

10.42 `rpki.config.parser` Class Reference

Inherits [object](#).

Public Member Functions

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

Public Attributes

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

Private Member Functions

- [def _get_wrapper](#)

10.42.1 Detailed Description

Extensions to stock Python ConfigParser:

Read config file and set default section while initializing parser object.

Support for OpenSSL-style subscripted options.

get-methods with default values and default section name.

Definition at line 38 of file config.py.

10.42.2 Member Function Documentation

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

Initialize this parser.

Definition at line 49 of file config.py.

10.42.2.2 **def** rpki.config.parser._get_wrapper (*self*, *method*, *section*, *option*, *default*) [private]

Wrapper method to add default value and default section support to ConfigParser methods.

Definition at line 98 of file config.py.

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

Get an option, perhaps with a default value.

Definition at line 111 of file config.py.

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

Get a boolean option, perhaps with a default value.

Definition at line 117 of file config.py.

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

Get an integer option, perhaps with a default value.

Definition at line 123 of file config.py.

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

Test whether an option exists.

Definition at line 70 of file config.py.

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

Test whether a section exists.

Definition at line 63 of file config.py.

10.42.2.8 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 79 of file config.py.

10.42.3 Member Data Documentation

10.42.3.1 rpki.config.parser.cfg

Definition at line 55 of file config.py.

10.42.3.2 rpki.config.parser.default_section

Definition at line 61 of file config.py.

10.42.3.3 rpki.config.parser.filename

Definition at line 54 of file config.py.

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

- [config.py \(2637\)](#)

10.43 rpki.exceptions.BadClassNameSyntax Class Reference

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

10.43.1 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 \(2742\)](#)

10.44 `rpki.exceptions.BadClientURL` Class Reference

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

10.44.1 Detailed Description

URL given to HTTPS client does not match profile.

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

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

- [exceptions.py \(2742\)](#)

10.45 `rpki.exceptions.BadContactURL` Class Reference

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

10.45.1 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 \(2742\)](#)

10.46 `rpki.exceptions.BadExtension` Class Reference

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

10.46.1 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 \(2742\)](#)

10.47 `rpki.exceptions.BadIRDBReply` Class Reference

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

10.47.1 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 \(2742\)](#)

10.48 `rpki.exceptions.BadIssueResponse` Class Reference

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

10.48.1 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 \(2742\)](#)

10.49 `rpki.exceptions.BadPKCS10` Class Reference

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

10.49.1 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 \(2742\)](#)

10.50 `rpki.exceptions.BadPublicationReply` Class Reference

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

10.50.1 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 \(2742\)](#)

10.51 `rpki.exceptions.BadQuery` Class Reference

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

10.51.1 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 \(2742\)](#)

10.52 `rpki.exceptions.BadSender` Class Reference

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

10.52.1 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 \(2742\)](#)

10.53 `rpki.exceptions.BadStatusCode` Class Reference

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

10.53.1 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 \(2742\)](#)

10.54 `rpki.exceptions.BadURISyntax` Class Reference

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

10.54.1 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 \(2742\)](#)

10.55 `rpki.exceptions.BSCNotFound` Class Reference

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

10.55.1 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 \(2742\)](#)

10.56 rpki.exceptions.BSCNotReady Class Reference

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

10.56.1 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 \(2742\)](#)

10.57 rpki.exceptions.ChildNotFound Class Reference

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

10.57.1 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 \(2742\)](#)

10.58 rpki.exceptions.ClassNameMismatch Class Reference

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

10.58.1 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 \(2742\)](#)

10.59 `rpki.exceptions.ClassNameUnknown` Class Reference

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

10.59.1 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 \(2742\)](#)

10.60 `rpki.exceptions.ClientNotFound` Class Reference

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

10.60.1 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 \(2742\)](#)

10.61 `rpki.exceptions.CMSCRLNotSet` Class Reference

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

10.61.1 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 \(2742\)](#)

10.62 `rpki.exceptions.CMSVerificationFailed` Class Reference

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

10.62.1 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 \(2742\)](#)

10.63 `rpki.exceptions.DBConsistencyError` Class Reference

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

10.63.1 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 \(2742\)](#)

10.64 `rpki.exceptions.DERObjectConversionError` Class Reference

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

10.64.1 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 \(2742\)](#)

10.65 `rpki.exceptions.DuplicateObject` Class Reference

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

10.65.1 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 \(2742\)](#)

10.66 `rpki.exceptions.EmptyPEM` Class Reference

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

10.66.1 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 \(2742\)](#)

10.67 `rpki.exceptions.EmptyROAPrefixList` Class Reference

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

10.67.1 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 \(2742\)](#)

10.68 `rpki.exceptions.ForbiddenURI` Class Reference

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

10.68.1 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 \(2742\)](#)

10.69 `rpki.exceptions.HandleTranslationError` Class Reference

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

10.69.1 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 \(2742\)](#)

10.70 `rpki.exceptions.HTTPRequestFailed` Class Reference

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

10.70.1 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 \(2742\)](#)

10.71 `rpki.exceptions.HTTPSBadVersion` Class Reference

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

10.71.1 Detailed Description

`HTTPS couldn't parse HTTP version.`

Definition at line 287 of file `exceptions.py`.

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

- [exceptions.py \(2742\)](#)

10.72 `rpki.exceptions.HTTPSClientAborted` Class Reference

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

10.72.1 Detailed Description

`HTTPS client connection closed while in request-sent state.`

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

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

- [exceptions.py \(2742\)](#)

10.73 `rpki.exceptions.HTTPSUnexpectedState` Class Reference

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

10.73.1 Detailed Description

`HTTPS event occurred in an unexpected state.`

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

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

- [exceptions.py \(2742\)](#)

10.74 `rpki.exceptions.MissingCMSCRL` Class Reference

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

10.74.1 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 \(2742\)](#)

10.75 `rpki.exceptions.MissingCMSEECert` Class Reference

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

10.75.1 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 \(2742\)](#)

10.76 `rpki.exceptions.MultipleTLSEECert` Class Reference

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

10.76.1 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 \(2742\)](#)

10.77 `rpki.exceptions.MustBePrefix` Class Reference

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

10.77.1 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 \(2742\)](#)

10.78 `rpki.exceptions.NoActiveCA` Class Reference

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

10.78.1 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 \(2742\)](#)

10.79 `rpki.exceptions.NoCoveringCertForROA` Class Reference

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

10.79.1 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 \(2742\)](#)

10.80 `rpki.exceptions.NoObjectAtURI` Class Reference

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

10.80.1 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 \(2742\)](#)

10.81 `rpki.exceptions.NotACertificateChain` Class Reference

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

10.81.1 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 \(2742\)](#)

10.82 `rpki.exceptions.NotFound` Class Reference

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

10.82.1 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 \(2742\)](#)

10.83 `rpki.exceptions.NotImplementedYet` Class Reference

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

10.83.1 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 \(2742\)](#)

10.84 `rpki.exceptions.NotInDatabase` Class Reference

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

10.84.1 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 \(2742\)](#)

10.85 `rpki.exceptions.ReceivedTLSCACert` Class Reference

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

10.85.1 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 \(2742\)](#)

10.86 rpki.exceptions.RPKI_Exception Class Reference

Inherits [Exception](#).

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

10.86.1 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 \(2742\)](#)

10.87 rpki.exceptions.ServerShuttingDown Class Reference

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

10.87.1 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 \(2742\)](#)

10.88 rpki.exceptions.SKIMismatch Class Reference

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

10.88.1 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 \(2742\)](#)

10.89 rpki.exceptions.SubprocessError Class Reference

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

10.89.1 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 \(2742\)](#)

10.90 rpki.exceptions.TLSValidationError Class Reference

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

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

10.90.1 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 \(2742\)](#)

10.91 rpki.exceptions.UnexpectedCMSCerts Class Reference

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

10.91.1 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 \(2742\)](#)

10.92 rpki.exceptions.UnexpectedCMSCRLs Class Reference

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

10.92.1 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 \(2742\)](#)

10.93 rpki.exceptions.UnparsableCMSDER Class Reference

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

10.93.1 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 \(2742\)](#)

10.94 rpki.exceptions.UpstreamError Class Reference

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

10.94.1 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 \(2742\)](#)

10.95 rpki.exceptions.WrongEContentType Class Reference

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

10.95.1 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 \(2742\)](#)

10.96 rpki.https.http_client Class Reference

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

Public Member Functions

- def `__init__`
- def `handle_close`
- def `handle_connect`
- def `handle_error`
- def `handle_message`
- def `handle_no_content_length`
- def `handle_timeout`
- def `send_request`
- def `set_state`
- def `start`
- def `tls_connect`

Public Attributes

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

Static Public Attributes

- `parse_type` = `http_response`
- `timeout` = `default_client_timeout`

10.96.1 Detailed Description

Definition at line 513 of file `https.py`.

10.96.2 Member Function Documentation

10.96.2.1 `def rpki.https.http_client.__init__ (self, queue, hostport, cert = None, key = None, ta = ())`

Definition at line 519 of file `https.py`.

10.96.2.2 def rpki.https.http_client.handle_close (*self*)

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

Definition at line 608 of file https.py.

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

Definition at line 540 of file https.py.

10.96.2.4 def rpki.https.http_client.handle_error (*self*)

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

Definition at line 623 of file https.py.

10.96.2.5 def rpki.https.http_client.handle_message (*self*)

Definition at line 581 of file https.py.

10.96.2.6 def rpki.https.http_client.handle_no_content_length (*self*)

Definition at line 570 of file https.py.

10.96.2.7 def rpki.https.http_client.handle_timeout (*self*)

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

Definition at line 617 of file https.py.

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

Definition at line 573 of file https.py.

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

Definition at line 566 of file https.py.

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

Definition at line 531 of file https.py.

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

Definition at line 554 of file https.py.

10.96.3 Member Data Documentation**10.96.3.1 rpki.https.http_client.cert**

Definition at line 527 of file https.py.

10.96.3.2 rpki.https.http_client.expect_close

Definition at line 526 of file https.py.

10.96.3.3 rpki.https.http_client.hostport

Definition at line 524 of file https.py.

10.96.3.4 rpki.https.http_client.key

Definition at line 528 of file https.py.

10.96.3.5 rpki.https.http_client.parse_type = http_response [static]

Definition at line 515 of file https.py.

10.96.3.6 rpki.https.http_client.queue

Definition at line 523 of file https.py.

10.96.3.7 rpki.https.http_client.retry_read

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

Definition at line 558 of file https.py.

10.96.3.8 rpki.https.http_client.retry_write

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

Definition at line 560 of file https.py.

10.96.3.9 rpki.https.http_client.state

Definition at line 525 of file https.py.

10.96.3.10 rpki.https.http_client.ta

Definition at line 529 of file https.py.

10.96.3.11 rpki.https.http_client.timeout = default_client_timeout [static]

Definition at line 517 of file https.py.

10.96.3.12 rpki.https.http_client.tls

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

Definition at line 542 of file https.py.

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

- [https.py \(2751\)](#)

10.97 rpki.https.http_listener Class Reference

Inherits [asyncore::dispatcher](#).

Public Member Functions

- [def __init__](#)
- [def handle_accept](#)
- [def handle_error](#)

Public Attributes

- [cert](#)
- [dynamic_ta](#)
- [handlers](#)
- [key](#)
- [ta](#)

Static Public Attributes

- [log](#) = logger

10.97.1 Detailed Description

Definition at line 471 of file https.py.

10.97.2 Member Function Documentation

10.97.2.1 `def rpki.https.http_listener.__init__(self, handlers, port = 80, host = "", cert = None, key = None, ta = None, dynamic_ta = None)`

Definition at line 475 of file https.py.

10.97.2.2 def rpki.https.http_listener.handle_accept (*self*)

Definition at line 496 of file https.py.

10.97.2.3 def rpki.https.http_listener.handle_error (*self*)

Definition at line 505 of file https.py.

10.97.3 Member Data Documentation

10.97.3.1 rpki.https.http_listener.cert

Definition at line 479 of file https.py.

10.97.3.2 rpki.https.http_listener.dynamic_ta

Definition at line 482 of file https.py.

10.97.3.3 rpki.https.http_listener.handlers

Definition at line 478 of file https.py.

10.97.3.4 rpki.https.http_listener.key

Definition at line 480 of file https.py.

10.97.3.5 rpki.https.http_listener.log = logger [static]

Definition at line 473 of file https.py.

10.97.3.6 rpki.https.http_listener.ta

Definition at line 481 of file https.py.

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

- [https.py \(2751\)](#)

10.98 rpki.https.http_message Class Reference

Inherits [object](#).

Inherited by [rpki.https.http_request](#), and [rpki.https.http_response](#).

Public Member Functions

- def [__init__](#)
- def [__str__](#)
- def [format](#)
- def [normalize_headers](#)
- def [parse_from_wire](#)
- def [parse_version](#)
- def [persistent](#)

Public Attributes

- [body](#)
- [headers](#)
- [version](#)

Static Public Attributes

- string [software_name](#) = "ISC RPKI library"

10.98.1 Detailed Description

Definition at line 67 of file https.py.

10.98.2 Member Function Documentation

10.98.2.1 `def rpki.https.http_message.__init__ (self, version = None, body = None, headers = None)`

Definition at line 71 of file https.py.

10.98.2.2 `def rpki.https.http_message.__str__ (self)`

Definition at line 119 of file https.py.

10.98.2.3 `def rpki.https.http_message.format (self)`

Definition at line 107 of file https.py.

10.98.2.4 `def rpki.https.http_message.normalize_headers (self, headers = None)`

Definition at line 77 of file https.py.

10.98.2.5 `def rpki.https.http_message.parse_from_wire (cls, headers)`

Definition at line 96 of file https.py.

10.98.2.6 `def rpki.https.http_message.parse_version (self, version)`

Definition at line 122 of file https.py.

10.98.2.7 `def rpki.https.http_message.persistent (self)`

Definition at line 127 of file https.py.

10.98.3 Member Data Documentation

10.98.3.1 rpki.https.http_message.body

Definition at line 73 of file https.py.

10.98.3.2 rpki.https.http_message.headers

Definition at line 74 of file https.py.

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

Definition at line 69 of file https.py.

10.98.3.4 rpki.https.http_message.version

Definition at line 72 of file https.py.

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

- [https.py \(2751\)](#)

10.99 rpki.https.http_queue Class Reference

Inherits [object](#).

Public Member Functions

- def [__init__](#)
- def [detach](#)
- def [request](#)
- def [restart](#)
- def [return_result](#)
- def [send_request](#)

Public Attributes

- [cert](#)
- [client](#)
- [hostport](#)
- [key](#)
- [queue](#)
- [ta](#)

Static Public Attributes

- [log](#) = logger

10.99.1 Detailed Description

Definition at line 628 of file https.py.

10.99.2 Member Function Documentation

10.99.2.1 `def rpki.https.http_queue.__init__ (self, hostport, cert = None, key = None, ta = ())`

Definition at line 632 of file https.py.

10.99.2.2 `def rpki.https.http_queue.detach (self, client)`

Definition at line 662 of file https.py.

10.99.2.3 `def rpki.https.http_queue.request (self, requests)`

Definition at line 642 of file https.py.

10.99.2.4 `def rpki.https.http_queue.restart (self)`

Definition at line 646 of file https.py.

10.99.2.5 `def rpki.https.http_queue.return_result (self, result)`

Definition at line 667 of file https.py.

10.99.2.6 `def rpki.https.http_queue.send_request (self)`

Definition at line 658 of file https.py.

10.99.3 Member Data Documentation**10.99.3.1** `rpki.https.http_queue.cert`

Definition at line 638 of file https.py.

10.99.3.2 `rpki.https.http_queue.client`

Definition at line 636 of file https.py.

10.99.3.3 `rpki.https.http_queue.hostport`

Definition at line 635 of file https.py.

10.99.3.4 `rpki.https.http_queue.key`

Definition at line 639 of file https.py.

10.99.3.5 `rpki.https.http_queue.log = logger` `[static]`

Definition at line 630 of file https.py.

10.99.3.6 rpki.https.http_queue.queue

Definition at line 637 of file https.py.

10.99.3.7 rpki.https.http_queue.ta

Definition at line 640 of file https.py.

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

- [https.py \(2751\)](#)

10.100 rpki.https.http_request Class Reference

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

Public Member Functions

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

Public Attributes

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

10.100.1 Detailed Description

Definition at line 136 of file https.py.

10.100.2 Member Function Documentation

10.100.2.1 `def rpki.https.http_request.__init__ (self, cmd = None, path = None, version = default_http_version, body = None, callback = None, errback = None, headers)`

Definition at line 138 of file https.py.

10.100.2.2 `def rpki.https.http_request.format_first_line (self)`

Definition at line 152 of file https.py.

10.100.2.3 `def rpki.https.http_request.parse_first_line (self, cmd, path, version)`

Definition at line 147 of file https.py.

10.100.3 Member Data Documentation

10.100.3.1 `rpki.https.http_request.callback`

Definition at line 143 of file https.py.

10.100.3.2 `rpki.https.http_request.cmd`

Definition at line 141 of file https.py.

10.100.3.3 `rpki.https.http_request.errback`

Definition at line 144 of file https.py.

10.100.3.4 rpki.https.http_request.path

Definition at line 142 of file https.py.

10.100.3.5 rpki.https.http_request.retried

Definition at line 145 of file https.py.

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

- [https.py \(2751\)](#)

10.101 rpki.https.http_response Class Reference

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

Public Member Functions

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

Public Attributes

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

10.101.1 Detailed Description

Definition at line 156 of file https.py.

10.101.2 Member Function Documentation

10.101.2.1 `def rpki.https.http_response.__init__ (self, code = None, reason = None, version = default_http_version, body = None, headers)`

Definition at line 158 of file https.py.

10.101.2.2 def rpki.https.http_response.format_first_line (*self*)

Definition at line 168 of file https.py.

10.101.2.3 def rpki.https.http_response.parse_first_line (*self*, *version*, *code*, *reason*)

Definition at line 163 of file https.py.

10.101.3 Member Data Documentation

10.101.3.1 rpki.https.http_response.code

Definition at line 160 of file https.py.

10.101.3.2 rpki.https.http_response.reason

Definition at line 161 of file https.py.

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

- [https.py \(2751\)](#)

10.102 rpki.https.http_server Class Reference

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

Public Member Functions

- def [__init__](#)
- def [find_handler](#)
- def [handle_message](#)
- def [handle_no_content_length](#)
- def [send_error](#)
- def [send_message](#)
- def [send_reply](#)
- def [tls_accept](#)

Public Attributes

- [expect_close](#)
- [handlers](#)
- [retry_read](#)
- [retry_write](#)
- [tls](#)

Static Public Attributes

- [parse_type](#) = [http_request](#)
- [timeout](#) = [default_server_timeout](#)

10.102.1 Detailed Description

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

10.102.2 Member Function Documentation

10.102.2.1 `def rpki.https.http_server.__init__ (self, sock, handlers, cert = None, key = None, ta = (), dynamic_ta = None)`

Definition at line 384 of file `https.py`.

10.102.2.2 `def rpki.https.http_server.find_handler (self, path)`

Helper method to search `self.handlers`.

Definition at line 417 of file `https.py`.

10.102.2.3 `def rpki.https.http_server.handle_message (self)`

Definition at line 426 of file `https.py`.

10.102.2.4 def rpki.https.http_server.handle_no_content_length (self)

Definition at line 414 of file https.py.

10.102.2.5 def rpki.https.http_server.send_error (self, code, reason)

Definition at line 449 of file https.py.

**10.102.2.6 def rpki.https.http_server.send_message (self, code, reason = "OK",
body = None)**

Definition at line 455 of file https.py.

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

Definition at line 452 of file https.py.

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

Definition at line 406 of file https.py.

10.102.3 Member Data Documentation**10.102.3.1 rpki.https.http_server.expect_close**

Definition at line 388 of file https.py.

10.102.3.2 rpki.https.http_server.handlers

Definition at line 386 of file https.py.

10.102.3.3 rpki.https.http_server.parse_type = http_request [static]

Definition at line 380 of file https.py.

10.102.3.4 rpki.https.http_server.retry_read

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

Definition at line 410 of file https.py.

10.102.3.5 rpki.https.http_server.retry_write

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

Definition at line 412 of file https.py.

10.102.3.6 rpki.https.http_server.timeout = default_server_timeout
[static]

Definition at line 382 of file https.py.

10.102.3.7 rpki.https.http_server.tls

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

Definition at line 392 of file https.py.

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

- [https.py \(2751\)](#)

10.103 rpki.https.http_stream Class Reference

Inherits [asyncchat::async_chat](#).

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

Public Member Functions

- def [__init__](#)
- def [chunk_body](#)
- def [chunk_discard_crlf](#)
- def [chunk_discard_trailer](#)
- def [chunk_header](#)
- def [close](#)
- def [collect_incoming_data](#)
- def [found_terminator](#)
- def [get_buffer](#)
- def [handle_body](#)
- def [handle_close](#)
- def [handle_error](#)
- def [handle_read](#)
- def [handle_timeout](#)
- def [handle_write](#)
- def [initiate_send](#)
- def [log_cert](#)
- def [readable](#)
- def [recv](#)
- def [restart](#)
- def [send](#)
- def [update_timeout](#)
- def [writable](#)

Public Attributes

- [buffer](#)
- [chunk_handler](#)
- [msg](#)
- [timer](#)

Static Public Attributes

- [log](#) = logger
- [retry_read](#) = None
- [retry_write](#) = None
- [tls](#) = None

10.103.1 Detailed Description

Definition at line 177 of file `https.py`.

10.103.2 Member Function Documentation

10.103.2.1 `def rpki.https.http_stream.__init__ (self, sock = None)`

Definition at line 184 of file https.py.

10.103.2.2 `def rpki.https.http_stream.chunk_body (self)`

Definition at line 244 of file https.py.

10.103.2.3 `def rpki.https.http_stream.chunk_discard_crlf (self)`

Definition at line 251 of file https.py.

10.103.2.4 `def rpki.https.http_stream.chunk_discard_trailer (self)`

Definition at line 257 of file https.py.

10.103.2.5 `def rpki.https.http_stream.chunk_header (self)`

Definition at line 234 of file https.py.

10.103.2.6 `def rpki.https.http_stream.close (self, force = False)`

Definition at line 358 of file https.py.

10.103.2.7 `def rpki.https.http_stream.collect_incoming_data (self, data)`

Buffer the data

Definition at line 205 of file https.py.

10.103.2.8 def rpki.https.http_stream.found_terminator (*self*)

Definition at line 217 of file https.py.

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

Definition at line 212 of file https.py.

10.103.2.10 def rpki.https.http_stream.handle_body (*self*)

Definition at line 264 of file https.py.

10.103.2.11 def rpki.https.http_stream.handle_close (*self*)

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

Definition at line 283 of file https.py.

10.103.2.12 def rpki.https.http_stream.handle_error (*self*)

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

Definition at line 268 of file https.py.

10.103.2.13 def rpki.https.http_stream.handle_read (*self*)

Definition at line 303 of file https.py.

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

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

Definition at line 279 of file https.py.

10.103.2.15 def rpki.https.http_stream.handle_write (*self*)

Definition at line 324 of file https.py.

10.103.2.16 def rpki.https.http_stream.initiate_send (*self*)

Definition at line 343 of file https.py.

10.103.2.17 def rpki.https.http_stream.log_cert (*self*, *tag*, *x*)

Definition at line 374 of file https.py.

10.103.2.18 def rpki.https.http_stream.readable (*self*)

Definition at line 297 of file https.py.

10.103.2.19 def rpki.https.http_stream.recv (*self*, *buffer_size*)

Definition at line 292 of file https.py.

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

Definition at line 190 of file https.py.

10.103.2.21 def rpki.https.http_stream.send (*self*, *data*)

Definition at line 287 of file https.py.

10.103.2.22 def rpki.https.http_stream.update_timeout (self)

Definition at line 199 of file https.py.

10.103.2.23 def rpki.https.http_stream.writeable (self)

Definition at line 300 of file https.py.

10.103.3 Member Data Documentation**10.103.3.1 rpki.https.http_stream.buffer**

Definition at line 186 of file https.py.

10.103.3.2 rpki.https.http_stream.chunk_handler

Definition at line 192 of file https.py.

10.103.3.3 rpki.https.http_stream.log = logger [static]

Definition at line 179 of file https.py.

10.103.3.4 rpki.https.http_stream.msg

Definition at line 224 of file https.py.

10.103.3.5 rpki.https.http_stream.retry_read = None [static]

Reimplemented in [rpki.https.http_server](#), and [rpki.https.http_client](#).

Definition at line 181 of file https.py.

10.103.3.6 rpki.https.http_stream.retry_write = None [static]

Reimplemented in [rpki.https.http_server](#), and [rpki.https.http_client](#).

Definition at line 182 of file https.py.

10.103.3.7 rpki.https.http_stream.timer

Definition at line 187 of file https.py.

10.103.3.8 rpki.https.http_stream.tls = None [static]

Reimplemented in [rpki.https.http_server](#), and [rpki.https.http_client](#).

Definition at line 180 of file https.py.

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

- [https.py \(2751\)](#)

10.104 rpki.ipaddrs.v4addr Class Reference

Inherits [long](#).

Public Member Functions

- def [__new__](#)
- def [__str__](#)
- def [from_bytes](#)
- def [to_bytes](#)

Static Public Attributes

- int [bits](#) = 32

10.104.1 Detailed Description

IPv4 address.

Derived from long, but supports IPv4 print syntax.

Definition at line 47 of file ipaddrs.py.

10.104.2 Member Function Documentation

10.104.2.1 def rpki.ipaddrs.v4addr.__new__ (cls, x)

Construct a v4addr object.

Definition at line 56 of file ipaddrs.py.

10.104.2.2 def rpki.ipaddrs.v4addr.__str__ (self)

Convert a v4addr object to string format.

Definition at line 74 of file ipaddrs.py.

10.104.2.3 def rpki.ipaddrs.v4addr.from_bytes (cls, x)

Convert from a raw byte string to a v4addr object.

Definition at line 70 of file ipaddrs.py.

10.104.2.4 def rpki.ipaddrs.v4addr.to_bytes (self)

Convert a v4addr object to a raw byte string.

Definition at line 65 of file ipaddrs.py.

10.104.3 Member Data Documentation

10.104.3.1 int rpki.ipaddrs.v4addr.bits = 32 [static]

Definition at line 54 of file ipaddrs.py.

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

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

10.105 rpki.ipaddrs.v6addr Class Reference

Inherits [long](#).

Public Member Functions

- def [__new__](#)
- def [__str__](#)
- def [from_bytes](#)
- def [to_bytes](#)

Static Public Attributes

- int [bits](#) = 128

10.105.1 Detailed Description

IPv6 address.

Derived from long, but supports IPv6 print syntax.

Definition at line 78 of file ipaddrs.py.

10.105.2 Member Function Documentation

10.105.2.1 def rpki.ipaddrs.v6addr.__new__(cls, x)

Construct a v6addr object.

Definition at line 87 of file ipaddrs.py.

10.105.2.2 def rpki.ipaddrs.v6addr.__str__ (self)

Convert a v6addr object to string format.

Definition at line 104 of file ipaddrs.py.

10.105.2.3 def rpki.ipaddrs.v6addr.from_bytes (cls, x)

Convert from a raw byte string to a v6addr object.

Definition at line 99 of file ipaddrs.py.

10.105.2.4 def rpki.ipaddrs.v6addr.to_bytes (self)

Convert a v6addr object to a raw byte string.

Definition at line 94 of file ipaddrs.py.

10.105.3 Member Data Documentation**10.105.3.1 int rpki.ipaddrs.v6addr.bits = 128 [static]**

Definition at line 85 of file ipaddrs.py.

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

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

10.106 rpki.left_right.bsc_elt Class Reference

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

Inherited by [irbe_cli.bsc_elt](#).

Public Member Functions

- def [children](#)
- def [parents](#)
- def [repositories](#)
- def [serve_pre_save_hook](#)

Static Public Attributes

- tuple [attributes](#) = ("action", "tag", "[self_handle](#)", "bsc_handle", "key_type", "hash_alg", "key_length")
XML attributes for this element.
- tuple [booleans](#) = ("generate_keypair",)
Boolean attributes (value "yes" or "no") for this element.
- string [element_name](#) = "bsc"
- tuple [elements](#) = ("signing_cert", "[signing_cert_crl](#)", "[pkcs10_request](#)")
XML elements contained by this element.
- tuple [handles](#) = (("self", self_elt),)
- [pkcs10_request](#) = None
- [private_key_id](#) = None
- [signing_cert](#) = None
- [signing_cert_crl](#) = None
- tuple [sql_template](#)

10.106.1 Detailed Description

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

Definition at line 542 of file `left_right.py`.

10.106.2 Member Function Documentation

10.106.2.1 def rpki.left_right.bsc_elt.children (*self*)

Fetch all child objects that link to this BSC object.

Definition at line 573 of file `left_right.py`.

10.106.2.2 def rpki.left_right.bsc_elt.parents (*self*)

Fetch all parent objects that link to this BSC object.

Definition at line 569 of file left_right.py.

10.106.2.3 def rpki.left_right.bsc_elt.repositories (*self*)

Fetch all repository objects that link to this BSC object.

Definition at line 565 of file left_right.py.

10.106.2.4 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 577 of file left_right.py.

10.106.3 Member Data Documentation

10.106.3.1 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 548 of file left_right.py.

10.106.3.2 `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 550 of file left_right.py.

10.106.3.3 `string rpki.left_right.bsc_elt.element_name = "bsc"` [static]

Definition at line 547 of file left_right.py.

10.106.3.4 `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 549 of file left_right.py.

10.106.3.5 `tuple rpki.left_right.bsc_elt.handles = (("self", self_elt),)`
[static]

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

Definition at line 558 of file left_right.py.

10.106.3.6 `rpki.left_right.bsc_elt.pkcs10_request = None` [static]

Definition at line 561 of file left_right.py.

10.106.3.7 `rpki.left_right.bsc_elt.private_key_id = None` [static]

Definition at line 560 of file left_right.py.

10.106.3.8 rpki.left_right.bsc_elt.signing_cert = None [static]

Reimplemented in [irbe_cli.bsc_elt](#).

Definition at line 562 of file left_right.py.

10.106.3.9 rpki.left_right.bsc_elt.signing_cert_crl = None [static]

Reimplemented in [irbe_cli.bsc_elt](#).

Definition at line 563 of file left_right.py.

10.106.3.10 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 552 of file left_right.py.

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

- [left_right.py \(2795\)](#)

10.107 rpki.left_right.child_elt Class Reference

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

Inherited by [irbe_cli.child_elt](#).

Public Member Functions

- def [ca_from_class_name](#)
- def [child_certs](#)
- def [endElement](#)
- def [parents](#)

- def [serve_destroy_hook](#)
- def [serve_post_save_hook](#)
- def [serve_up_down](#)

Static Public Attributes

- tuple [attributes](#) = ("action", "tag", "[self_handle](#)", "child_handle", "bsc_handle")

XML attributes for this element.

- tuple [booleans](#) = ("reissue",)

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

- [bpki_cert](#) = None
- [bpki_glue](#) = None
- [clear_https_ta_cache](#) = False
- string [element_name](#) = "child"
- tuple [elements](#) = ("bpki_cert", "[bpki_glue](#)")

XML elements contained by this element.

- tuple [handles](#) = (("self", self_elt), ("bsc", bsc_elt))
- tuple [sql_template](#)

10.107.1 Detailed Description

<child/> element.

Definition at line 821 of file left_right.py.

10.107.2 Member Function Documentation

10.107.2.1 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 850 of file left_right.py.

10.107.2.2 `def rpki.left_right.child_elt.child_certs (self, ca_detail = None, ski = None, unique = False)`

Fetch all child_cert objects that link to this child object.

Definition at line 842 of file left_right.py.

10.107.2.3 `def rpki.left_right.child_elt.endElement (self, stack, name, text)`

Handle subelements of <child/> element. These require special handling because modifying them invalidates the HTTPS trust anchor cache.

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

Definition at line 882 of file left_right.py.

10.107.2.4 `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 846 of file left_right.py.

10.107.2.5 `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 874 of file left_right.py.

10.107.2.6 `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 864 of file left_right.py.

10.107.2.7 def rpki.left_right.child_elt.serve_up_down (self, query, callback)

Outer layer of server handling for one up-down PDU from this child.

Definition at line 892 of file left_right.py.

10.107.3 Member Data Documentation

10.107.3.1 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 827 of file left_right.py.

10.107.3.2 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 829 of file left_right.py.

10.107.3.3 rpki.left_right.child_elt.bpkcert = None [static]

Definition at line 838 of file left_right.py.

10.107.3.4 rpki.left_right.child_elt.bpkglue = None [static]

Definition at line 839 of file left_right.py.

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

Definition at line 840 of file left_right.py.

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

Definition at line 826 of file left_right.py.

10.107.3.7 tuple rpki.left_right.child_elt.elements = ("bpki_cert", "bpki_glue") [static]

XML elements contained by this element.

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

Definition at line 828 of file left_right.py.

10.107.3.8 tuple rpki.left_right.child_elt.handles = ("self", self_elt), ("bsc", bsc_elt)) [static]

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

Definition at line 836 of file left_right.py.

10.107.3.9 tuple rpki.left_right.child_elt.sql_template [static]

Initial value:

```
rpki.sql.template("child", "child_id", "child_handle",
                  "self_id", "bsc_id",
                  ("bpki_cert", rpki.x509.X509),
                  ("bpki_glue", rpki.x509.X509))
```

Definition at line 831 of file left_right.py.

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

- [left_right.py \(2795\)](#)

10.108 rpki.left_right.cms_msg Class Reference

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

Inherited by [irbe_cli.left_right_cms_msg](#).

Static Public Attributes

- string [encoding](#) = "us-ascii"
- [saxify](#) = sax_handler.saxify
- [schema](#) = [rpki.relaxng.left_right](#)

10.108.1 Detailed Description

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

Definition at line 1095 of file [left_right.py](#).

10.108.2 Member Data Documentation

10.108.2.1 string [rpki.left_right.cms_msg.encoding](#) = "us-ascii" [static]

Definition at line 1100 of file [left_right.py](#).

10.108.2.2 [rpki.left_right.cms_msg.saxify](#) = [sax_handler.saxify](#) [static]

Reimplemented in [irbe_cli.left_right_cms_msg](#).

Definition at line 1102 of file [left_right.py](#).

10.108.2.3 [rpki.left_right.cms_msg.schema](#) = [rpki.relaxng.left_right](#) [static]

Definition at line 1101 of file [left_right.py](#).

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

- [left_right.py \(2795\)](#)

10.109 rpki.left_right.data_elt Class Reference

Inherits [rpki::xml_utils::data_elt](#), [rpki::sql::sql_persistent](#), and [rpki::left_right::left_right_namespace](#).

Inherited by [rpki.left_right.bsc_elt](#), [rpki.left_right.child_elt](#), [rpki.left_right.parent_elt](#), [rpki.left_right.repository_elt](#), and [rpki.left_right.self_elt](#).

Public Member Functions

- def [bsc](#)
- def [make_reply_clone_hook](#)
- def [self](#)
- def [serve_fetch_all](#)
- def [serve_fetch_handle](#)
- def [serve_fetch_one_maybe](#)
- def [serve_pre_save_hook](#)

Static Public Attributes

- tuple [handles](#) = ()
- [self_handle](#) = None
- [self_id](#) = None

10.109.1 Detailed Description

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

Definition at line 50 of file [left_right.py](#).

10.109.2 Member Function Documentation

10.109.2.1 def rpki.left_right.data_elt.bsc (*self*)

Return BSC object to which this object links.

Definition at line 64 of file [left_right.py](#).

10.109.2.2 `def rpki.left_right.data_elt.make_reply_clone_hook (self, r_pdu)`

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

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

Definition at line 68 of file `left_right.py`.

10.109.2.3 `def rpki.left_right.data_elt.self (self)`

Fetch self object to which this object links.

Definition at line 60 of file `left_right.py`.

10.109.2.4 `def rpki.left_right.data_elt.serve_fetch_all (self)`

Find the objects on which a list method should operate.

Reimplemented in [rpki.left_right.self_elt](#).

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

10.109.2.5 `def rpki.left_right.data_elt.serve_fetch_handle (cls, gctx, self_id, handle)`

Find an object based on its handle.

Reimplemented in [rpki.left_right.self_elt](#).

Definition at line 84 of file `left_right.py`.

10.109.2.6 `def rpki.left_right.data_elt.serve_fetch_one_maybe (self)`

Find the object on which a get, set, or destroy method should operate, or which would conflict with a create method.

Reimplemented in [rpki.left_right.self_elt](#).

Definition at line 90 of file left_right.py.

10.109.2.7 def rpki.left_right.data_elt.serve_pre_save_hook (self, q_pdu, r_pdu, cb, eb)

Hook to do _handle => _id translation before saving.

self is always the object to be saved to SQL. For create operations, self and q_pdu are be the same object; for set operations, self is the pre-existing object from SQL and q_pdu is the set request received from the the IRBE.

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

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

Definition at line 106 of file left_right.py.

10.109.3 Member Data Documentation

10.109.3.1 tuple rpki.left_right.data_elt.handles = () [static]

Reimplemented in [rpki.left_right.self_elt](#), [rpki.left_right.bsc_elt](#), [rpki.left_right.repository_elt](#), [rpki.left_right.parent_elt](#), and [rpki.left_right.child_elt](#).

Definition at line 55 of file left_right.py.

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

Definition at line 58 of file left_right.py.

10.109.3.3 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 \(2795\)](#)

10.110 rpki.left_right.left_right_namespace Class Reference

Inherits [object](#).

Inherited by [rpki.left_right.data_elt](#), [rpki.left_right.list_published_objects_elt](#), [rpki.left_right.list_resources_elt](#), [rpki.left_right.list_roa_requests_elt](#), [rpki.left_right.msg](#), and [rpki.left_right.report_error_elt](#).

Static Public Attributes

- dictionary [nsmap](#) = { None : [xmlns](#) }
- string [xmlns](#) = "http://www.hactrn.net/uris/rpki/left-right-spec/"

10.110.1 Detailed Description

XML namespace parameters for left-right protocol.

Definition at line 42 of file [left_right.py](#).

10.110.2 Member Data Documentation

10.110.2.1 dictionary [rpki.left_right.left_right_namespace.nsmap](#) = { None : [xmlns](#) } [static]

Definition at line 48 of file [left_right.py](#).

10.110.2.2 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 \(2795\)](#)

10.111 rpki.left_right.list_published_objects_elt Class Reference

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

Inherited by [irbe_cli.list_published_objects_elt](#).

Public Member Functions

- def [make_reply](#)
- def [serve_dispatch](#)

Static Public Attributes

- tuple [attributes](#) = ("self_handle", "tag", "uri")
XML attributes for this element.
- string [element_name](#) = "list_published_objects"
- [obj](#) = None
- string [text_attribute](#) = "obj"
Name of the class attribute that holds the text value.

10.111.1 Detailed Description

`<list_published_objects/>` element.

Definition at line 984 of file `left_right.py`.

10.111.2 Member Function Documentation

10.111.2.1 def rpki.left_right.list_published_objects_elt.make_reply (*self*, *uri*, *obj*)

Generate one reply PDU.

Definition at line 1011 of file `left_right.py`.

10.111.2.2 `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 995 of file `left_right.py`.

10.111.3 Member Data Documentation

10.111.3.1 `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 990 of file `left_right.py`.

10.111.3.2 `string rpki.left_right.list_published_objects_elt.element_name = "list_published_objects" [static]`

Definition at line 989 of file `left_right.py`.

10.111.3.3 `rpki.left_right.list_published_objects_elt.obj = None [static]`

Definition at line 993 of file `left_right.py`.

10.111.3.4 `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 991 of file `left_right.py`.

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

- [left_right.py \(2795\)](#)

10.112 rpki.left_right.list_resources_elt Class Reference

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

Public Member Functions

- def [startElement](#)
- def [toXML](#)

Public Attributes

- [asn](#)
- [ipv4](#)
- [ipv6](#)

Static Public Attributes

- tuple [attributes](#) = ("self_handle", "tag", "child_handle", "[valid_until](#)", "[asn](#)", "[ipv4](#)", "[ipv6](#)")

XML attributes for this element.

- string [element_name](#) = "list_resources"
- [valid_until](#) = None

10.112.1 Detailed Description

`<list_resources/> element.`

Definition at line 929 of file `left_right.py`.

10.112.2 Member Function Documentation

10.112.2.1 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 938 of file left_right.py.

10.112.2.2 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 954 of file left_right.py.

10.112.3 Member Data Documentation

10.112.3.1 rpki.left_right.list_resources_elt.asn

Definition at line 948 of file left_right.py.

```
10.112.3.2 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 935 of file left_right.py.

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

Definition at line 934 of file left_right.py.

10.112.3.4 rpki.left_right.list_resources_elt.ipv4

Definition at line 950 of file left_right.py.

10.112.3.5 rpki.left_right.list_resources_elt.ipv6

Definition at line 952 of file left_right.py.

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

Definition at line 936 of file left_right.py.

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

- [left_right.py \(2795\)](#)

10.113 rpki.left_right.list_roa_requests_elt Class Reference

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

Public Member Functions

- def [startElement](#)

Public Attributes

- [ipv4](#)
- [ipv6](#)

Static Public Attributes

- tuple [attributes](#) = ("self_handle", "tag", "asn", "[ipv4](#)", "[ipv6](#)")
XML attributes for this element.
- string [element_name](#) = "list_roa_requests"

10.113.1 Detailed Description

<list_roa_requests/> element.

Definition at line 964 of file left_right.py.

10.113.2 Member Function Documentation

10.113.2.1 `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 972 of file left_right.py.

10.113.3 Member Data Documentation

10.113.3.1 `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 970 of file left_right.py.

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

Definition at line 969 of file left_right.py.

10.113.3.3 `rpki.left_right.list_roa_requests_elt.ipv4`

Definition at line 980 of file left_right.py.

10.113.3.4 rpki.left_right.list_roa_requests_elt.ipv6

Definition at line 982 of file left_right.py.

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

- [left_right.py \(2795\)](#)

10.114 rpki.left_right.msg Class Reference

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

Inherited by [irbe_cli.left_right_msg](#).

Public Member Functions

- def [serve_top_level](#)

Static Public Attributes

- tuple [pdus](#)
Dispatch table of PDUs for this protocol.
- int [version](#) = 1
Protocol version.

10.114.1 Detailed Description

Left-right PDU.

Definition at line 1042 of file left_right.py.

10.114.2 Member Function Documentation

10.114.2.1 def rpki.left_right.msg.serve_top_level (self, gctx, cb)

Serve one msg PDU.

Definition at line 1058 of file left_right.py.

10.114.3 Member Data Documentation

10.114.3.1 rpki::left_right.msg::pdus [static]

Initial value:

```
dict((x.element_name, x)
      for x in (self_elt, child_elt, parent_elt, bsc_elt, repository_elt,
               list_resources_elt, list_roa_requests_elt, list_published
               _objects_elt,
               report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented in [irbe_cli.left_right_msg](#).

Definition at line 1053 of file left_right.py.

10.114.3.2 rpki::left_right.msg::version = 1 [static]

Protocol version.

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

Definition at line 1049 of file left_right.py.

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

- [left_right.py \(2795\)](#)

10.115 rpki.left_right.parent_elt Class Reference

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

Inherited by [irbe_cli.parent_elt](#).

Public Member Functions

- def [cas](#)
- def [query_up_down](#)
- def [repository](#)
- def [serve_post_save_hook](#)
- def [serve_rekey](#)

- def [serve_revoke](#)
- def [serve_revoke_forgotten](#)

Static Public Attributes

- tuple [attributes](#)
XML attributes for this element.
- tuple [booleans](#) = ("rekey", "reissue", "revoke", "revoke_forgotten")
Boolean attributes (value "yes" or "no") for this element.
- [bpki_cms_cert](#) = None
- [bpki_cms_glue](#) = None
- [bpki_https_cert](#) = None
- [bpki_https_glue](#) = None
- string [element_name](#) = "parent"
- tuple [elements](#) = ("bpki_cms_cert", "bpki_cms_glue", "bpki_https_cert", "bpki_https_glue")
XML elements contained by this element.
- tuple [handles](#) = (("self", self_elt), ("bsc", bsc_elt), ("repository", repository_elt))
- tuple [sql_template](#)

10.115.1 Detailed Description

<parent/> element.

Definition at line 672 of file left_right.py.

10.115.2 Member Function Documentation

10.115.2.1 def rpki.left_right.parent_elt.cas (self)

Fetch all CA objects that link to this parent object.

Definition at line 699 of file left_right.py.

10.115.2.2 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 775 of file left_right.py.

10.115.2.3 def rpki.left_right.parent_elt.repository (self)

Fetch repository object to which this parent object links.

Definition at line 695 of file left_right.py.

10.115.2.4 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 703 of file left_right.py.

10.115.2.5 def rpki.left_right.parent_elt.serve_rekey (self, cb, eb)

Handle a left-right rekey action for this parent.

Definition at line 719 of file left_right.py.

10.115.2.6 def rpki.left_right.parent_elt.serve_revoke (self, cb, eb)

Handle a left-right revoke action for this parent.

Definition at line 727 of file left_right.py.

10.115.2.7 def rpki.left_right.parent_elt.serve_revoke_forgotten (self, cb, eb)

Handle a left-right revoke_forgotten action for this parent.

This is a bit fiddly: we have to compare the result of an up-down list query with what we have locally and identify the SKIs of any certificates that have gone missing. This should never happen in ordinary operation, but can arise if we have somehow lost a private key, in which case there is nothing more we can do with the issued cert, so we have to clear it. As this really is not supposed to happen, we don't clear it automatically, instead we require an explicit trigger.

Definition at line 735 of file left_right.py.

10.115.3 Member Data Documentation**10.115.3.1 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 678 of file left_right.py.

10.115.3.2 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 681 of file left_right.py.

10.115.3.3 rpki.left_right.parent_elt.bpkg_cms_cert = None [static]

Definition at line 690 of file left_right.py.

10.115.3.4 `rpki.left_right.parent_elt.bpki_cms_glue = None` `[static]`

Definition at line 691 of file left_right.py.

10.115.3.5 `rpki.left_right.parent_elt.bpki_https_cert = None` `[static]`

Definition at line 692 of file left_right.py.

10.115.3.6 `rpki.left_right.parent_elt.bpki_https_glue = None` `[static]`

Definition at line 693 of file left_right.py.

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

Definition at line 677 of file left_right.py.

10.115.3.8 `tuple rpki.left_right.parent_elt.elements = ("bpki_cms_cert",`
`"bpki_cms_glue", "bpki_https_cert", "bpki_https_glue")`
`[static]`

XML elements contained by this element.

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

Definition at line 680 of file left_right.py.

10.115.3.9 `tuple rpki.left_right.parent_elt.handles = ("self", self_elt), ("bsc",`
`bsc_elt), ("repository", repository_elt))` `[static]`

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

Definition at line 688 of file left_right.py.

10.115.3.10 tuple rpki.left_right.parent_elt.sql_template [static]

Initial value:

```
rpki.sql.template("parent", "parent_id", "parent_handle",
                  "self_id", "bsc_id", "repository_id",
                  ("bpki_cms_cert", rpki.x509.X509), ("bpki_cms_
glue", rpki.x509.X509),
                  ("bpki_https_cert", rpki.x509.X509), ("bpki_ht
tps_glue", rpki.x509.X509),
                  "peer_contact_uri", "sia_base", "sender_name",
                  "recipient_name")
```

Definition at line 683 of file left_right.py.

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

- [left_right.py \(2795\)](#)

10.116 rpki.left_right.report_error_elt Class Reference

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

Inherited by [irbe_cli.report_error_elt](#).

Public Member Functions

- def [from_exception](#)

Public Attributes

- [error_code](#)
- [self_handle](#)
- [tag](#)

Static Public Attributes

- tuple [attributes](#) = ("tag", "self_handle", "error_code")
XML attributes for this element.
- string [element_name](#) = "report_error"

- `error_text` = None
- string `text_attribute` = "error_text"
Name of the class attribute that holds the text value.

10.116.1 Detailed Description

`<report_error/>` element.

Definition at line 1019 of file `left_right.py`.

10.116.2 Member Function Documentation

10.116.2.1 `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 1031 of file `left_right.py`.

10.116.3 Member Data Documentation

10.116.3.1 `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 1025 of file `left_right.py`.

10.116.3.2 `string rpki.left_right.report_error_elt.element_name = "report_error" [static]`

Definition at line 1024 of file `left_right.py`.

10.116.3.3 `rpki.left_right.report_error_elt.error_code`

Definition at line 1038 of file `left_right.py`.

10.116.3.4 `rpki.left_right.report_error_elt.error_text = None` `[static]`

Definition at line 1028 of file `left_right.py`.

10.116.3.5 `rpki.left_right.report_error_elt.self_handle`

Definition at line 1036 of file `left_right.py`.

10.116.3.6 `rpki.left_right.report_error_elt.tag`

Definition at line 1037 of file `left_right.py`.

10.116.3.7 `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 1026 of file `left_right.py`.

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

- [left_right.py \(2795\)](#)

10.117 `rpki.left_right.repository_elt` Class Reference

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

Inherited by [irbe_cli.repository_elt](#).

Public Member Functions

- def [call_pubd](#)
- def [parents](#)
- def [publish](#)
- def [withdraw](#)

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](#)

10.117.1 Detailed Description

`<repository/>` element.

Definition at line 589 of file `left_right.py`.

10.117.2 Member Function Documentation

10.117.2.1 `def rpki.left_right.repository_elt.call_pubd (self, callback, errback, pdus)`

Send a message to publication daemon and return the response.

Definition at line 610 of file `left_right.py`.

10.117.2.2 def rpki.left_right.repository_elt.parents (self)

Fetch all parent objects that link to this repository object.

Definition at line 606 of file left_right.py.

10.117.2.3 def rpki.left_right.repository_elt.publish (self, obj, uri, callback, errback)

Publish one object in the repository.

Definition at line 647 of file left_right.py.

10.117.2.4 def rpki.left_right.repository_elt.withdraw (self, obj, uri, callback, errback, allow_failure = False)

Withdraw one object from the repository.

Definition at line 658 of file left_right.py.

10.117.3 Member Data Documentation**10.117.3.1 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 595 of file left_right.py.

10.117.3.2 rpki.left_right.repository_elt.bpki_cert = None [static]

Definition at line 603 of file left_right.py.

10.117.3.3 rpki.left_right.repository_elt.bpki_glue = None [static]

Definition at line 604 of file left_right.py.

10.117.3.4 string rpki.left_right.repository_elt.element_name = "repository"
[static]

Definition at line 594 of file left_right.py.

**10.117.3.5 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 596 of file left_right.py.

**10.117.3.6 tuple rpki.left_right.repository_elt.handles = (("self", self_elt),
("bsc", bsc_elt))** [static]

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

Definition at line 601 of file left_right.py.

10.117.3.7 tuple rpki.left_right.repository_elt.sql_template [static]**Initial value:**

```
rpki.sql.template("repository", "repository_id", "repository_handle",  
                  "self_id", "bsc_id", "peer_contact_uri",  
                  ("bpki_cert", rpki.x509.X509), ("bpki_glue", r  
pki.x509.X509))
```

Definition at line 598 of file left_right.py.

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

- [left_right.py \(2795\)](#)

10.118 rpki.left_right.sax_handler Class Reference

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

Inherited by [irbe_cli.left_right_sax_handler](#).

Static Public Attributes

- string [name](#) = "msg"
- [pdu](#) = [msg](#)
- string [version](#) = "1"

10.118.1 Detailed Description

SAX handler for Left-Right protocol.

Definition at line 1086 of file [left_right.py](#).

10.118.2 Member Data Documentation

10.118.2.1 string [rpki.left_right.sax_handler.name](#) = "msg" [static]

Definition at line 1092 of file [left_right.py](#).

10.118.2.2 [rpki.left_right.sax_handler.pdu](#) = [msg](#) [static]

Reimplemented in [irbe_cli.left_right_sax_handler](#).

Definition at line 1091 of file [left_right.py](#).

10.118.2.3 string [rpki.left_right.sax_handler.version](#) = "1" [static]

Definition at line 1093 of file [left_right.py](#).

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

- [left_right.py](#) (2795)

10.119 rpki.left_right.self_elt Class Reference

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

Inherited by [irbe_cli.self_elt](#).

Public Member Functions

- def [bscs](#)
- def [children](#)
- def [client_poll](#)
- def [cron](#)
- def [parents](#)
- def [regenerate_crls_and_manifests](#)
- def [repositories](#)
- def [roas](#)
- def [serve_fetch_all](#)
- def [serve_fetch_handle](#)
- def [serve_fetch_one_maybe](#)
- def [serve_post_save_hook](#)
- def [serve_publish_world_now](#)
- def [serve_rekey](#)
- def [serve_revoke](#)
- def [serve_revoke_forgotten](#)
- def [serve_run_now](#)
- def [update_children](#)
- def [update_roas](#)

Static Public Attributes

- tuple [attributes](#) = ("action", "tag", "self_handle", "crl_interval", "regen_margin")

XML attributes for this element.

- tuple [booleans](#) = ("rekey", "reissue", "revoke", "run_now", "publish_world_now", "revoke_forgotten")

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

- [bpki_cert](#) = None
- [bpki_glue](#) = None
- [crl_interval](#) = None
- string [element_name](#) = "self"
- tuple [elements](#) = ("bpki_cert", "bpki_glue")

XML elements contained by this element.

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

10.119.1 Detailed Description

`<self/> element.`

Definition at line 124 of file `left_right.py`.

10.119.2 Member Function Documentation

10.119.2.1 `def rpki.left_right.self_elt.bscs (self)`

Fetch all BSC objects that link to this self object.

Definition at line 145 of file `left_right.py`.

10.119.2.2 `def rpki.left_right.self_elt.children (self)`

Fetch all child objects that link to this self object.

Definition at line 157 of file `left_right.py`.

10.119.2.3 `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 300 of file `left_right.py`.

10.119.2.4 def rpki.left_right.self_elt.cron (*self*, *cb*)

Periodic tasks.

Definition at line 277 of file left_right.py.

10.119.2.5 def rpki.left_right.self_elt.parents (*self*)

Fetch all parent objects that link to this self object.

Definition at line 153 of file left_right.py.

10.119.2.6 def rpki.left_right.self_elt.regenerate_crls_and_manifests (*self*, *cb*)

Generate new CRLs and manifests as necessary for all of this self's CAs. Extracting nextUpdate from a manifest is hard at the moment due to implementation silliness, so for now we generate a new manifest whenever we generate a new CRL

This method also cleans up tombstones left behind by revoked ca_detail objects, since we're walking through the relevant portions of the database anyway.

Definition at line 436 of file left_right.py.

10.119.2.7 def rpki.left_right.self_elt.repositories (*self*)

Fetch all repository objects that link to this self object.

Definition at line 149 of file left_right.py.

10.119.2.8 def rpki.left_right.self_elt.roas (*self*)

Fetch all ROA objects that link to this self object.

Definition at line 161 of file left_right.py.

10.119.2.9 def rpki.left_right.self_elt.serve_fetch_all (self)

Find the self objects upon which a list action should operate.
This is different from the list action for all other objects,
where list only works within a given self_id context.

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

Definition at line 269 of file left_right.py.

10.119.2.10 def rpki.left_right.self_elt.serve_fetch_handle (cls, gctx, self_id, self_handle)

Find a self object based on its self_handle.

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

Definition at line 263 of file left_right.py.

10.119.2.11 def rpki.left_right.self_elt.serve_fetch_one_maybe (self)

Find the self object upon which a get, set, or destroy action
should operate, or which would conflict with a create method.

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

Definition at line 255 of file left_right.py.

10.119.2.12 def rpki.left_right.self_elt.serve_post_save_hook (self, q_pdu, r_pdu, cb, eb)

Extra server actions for self_elt.

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

Definition at line 165 of file left_right.py.

10.119.2.13 def rpki.left_right.self_elt.serve_publish_world_now (self, cb, eb)

Handle a left-right publish_world_now action for this self.

The publication stuff needs refactoring, right now publication is interleaved with local operations in a way that forces far too many bounces through the task system for any complex update. The whole thing ought to be rewritten to queue up outgoing publication PDUs and only send them when we're all done or when we need to force publication at a particular point in a multi-phase operation.

Once that reorganization has been done, this method should be rewritten to reuse the low-level publish() methods that each object will have...but we're not there yet. So, for now, we just do this via brute force. Think of it as a trial version to see whether we've identified everything that needs to be republished for this operation.

Definition at line 213 of file left_right.py.

10.119.2.14 def rpki.left_right.self_elt.serve_rekey (self, cb, eb)

Handle a left-right rekey action for this self.

Definition at line 186 of file left_right.py.

10.119.2.15 def rpki.left_right.self_elt.serve_revoke (self, cb, eb)

Handle a left-right revoke action for this self.

Definition at line 195 of file left_right.py.

10.119.2.16 def rpki.left_right.self_elt.serve_revoke_forgotten (self, cb, eb)

Handle a left-right revoke_forgotten action for this self.

Definition at line 204 of file left_right.py.

10.119.2.17 `def rpki.left_right.self_elt.serve_run_now (self, cb, eb)`

Handle a left-right run_now action for this self.

Definition at line 248 of file left_right.py.

10.119.2.18 `def rpki.left_right.self_elt.update_children (self, cb)`

Check for updated IRDB data for all of this self's children and issue new certs as necessary. Must handle changes both in resources and in expiration date.

Definition at line 354 of file left_right.py.

10.119.2.19 `def rpki.left_right.self_elt.update_roas (self, cb)`

Generate or update ROAs for this self.

Definition at line 487 of file left_right.py.

10.119.3 Member Data Documentation**10.119.3.1** `tuple rpki.left_right.self_elt.attributes = ("action", "tag", "self_handle", "crl_interval", "regen_margin") [static]`

XML attributes for this element.

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

Definition at line 130 of file left_right.py.

10.119.3.2 `tuple rpki.left_right.self_elt.booleans = ("rekey", "reissue", "revoke", "run_now", "publish_world_now", "revoke_forgotten") [static]`

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

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

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

10.119.3.3 `rpki.left_right.self_elt.bpki_cert = None` [static]

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

10.119.3.4 `rpki.left_right.self_elt.bpki_glue = None` [static]

Definition at line 143 of file `left_right.py`.

10.119.3.5 `rpki.left_right.self_elt.crl_interval = None` [static]

Definition at line 140 of file `left_right.py`.

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

Definition at line 129 of file `left_right.py`.

10.119.3.7 `tuple rpki.left_right.self_elt.elements = ("bpki_cert", "bpki_glue")` [static]

XML elements contained by this element.

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

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

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

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

Definition at line 137 of file left_right.py.

10.119.3.9 rpki.left_right.self_elt.regen_margin = None [static]

Definition at line 141 of file left_right.py.

10.119.3.10 tuple rpki.left_right.self_elt.sql_template [static]

Initial value:

```
rpki.sql.template("self", "self_id", "self_handle",  
                  "use_hsm", "crl_interval", "regen_margin",  
                  ("bpki_cert", rpki.x509.X509), ("bpki_glue", r  
                  pki.x509.X509))
```

Definition at line 134 of file left_right.py.

10.119.3.11 rpki.left_right.self_elt.use_hsm = False [static]

Definition at line 139 of file left_right.py.

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

- [left_right.py \(2795\)](#)

10.120 rpki.log.logger Class Reference

Inherits [object](#).

Public Member Functions

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

Public Attributes

- [priority](#)

10.120.1 Detailed Description

Closure for logging.

Definition at line 71 of file log.py.

10.120.2 Member Function Documentation

10.120.2.1 def rpki.log.logger.__call__ (*self*, *message*)

Definition at line 79 of file log.py.

10.120.2.2 def rpki.log.logger.__init__ (*self*, *priority*)

Definition at line 76 of file log.py.

10.120.3 Member Data Documentation

10.120.3.1 rpki.log.logger.priority

Definition at line 77 of file log.py.

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

- [log.py \(2732\)](#)

10.121 rpki.manifest.FileAndHash Class Reference

Inherits [Sequence](#).

Public Member Functions

- def [__init__](#)

Public Attributes

- [file](#)
- [hash](#)

10.121.1 Detailed Description

Definition at line 27 of file manifest.py.

10.121.2 Member Function Documentation

10.121.2.1 `def rpki.manifest.FileAndHash.__init__ (self, optional = 0, default = "")`

Definition at line 28 of file manifest.py.

10.121.3 Member Data Documentation

10.121.3.1 `rpki.manifest.FileAndHash.file`

Definition at line 29 of file manifest.py.

10.121.3.2 `rpki.manifest.FileAndHash.hash`

Definition at line 30 of file manifest.py.

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

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

10.122 rpki.manifest.FilesAndHashes Class Reference

Inherits [SequenceOf](#).

Public Member Functions

- `def __init__`

10.122.1 Detailed Description

Definition at line 34 of file manifest.py.

10.122.2 Member Function Documentation

10.122.2.1 `def rpki.manifest.FilesAndHashes.__init__ (self, optional = 0, default = "")`

Definition at line 35 of file manifest.py.

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

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

10.123 rpki.manifest.Manifest Class Reference

Inherits [Sequence](#).

Public Member Functions

- `def __init__`

Public Attributes

- [explicitVersion](#)
- [fileHashAlg](#)
- [fileList](#)
- [manifestNumber](#)
- [nextUpdate](#)
- [thisUpdate](#)
- [version](#)

10.123.1 Detailed Description

Definition at line 38 of file manifest.py.

10.123.2 Member Function Documentation

10.123.2.1 `def rpki.manifest.Manifest.__init__ (self, optional = 0, default = "")`

Definition at line 39 of file manifest.py.

10.123.3 Member Data Documentation**10.123.3.1 rpki.manifest.Manifest.explicitVersion**

Definition at line 41 of file manifest.py.

10.123.3.2 rpki.manifest.Manifest.fileHashAlg

Definition at line 45 of file manifest.py.

10.123.3.3 rpki.manifest.Manifest.fileList

Definition at line 46 of file manifest.py.

10.123.3.4 rpki.manifest.Manifest.manifestNumber

Definition at line 42 of file manifest.py.

10.123.3.5 rpki.manifest.Manifest.nextUpdate

Definition at line 44 of file manifest.py.

10.123.3.6 rpki.manifest.Manifest.thisUpdate

Definition at line 43 of file manifest.py.

10.123.3.7 rpki.manifest.Manifest.version

Definition at line 40 of file manifest.py.

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

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

10.124 rpki.publication.certificate_elt Class Reference

Inherits [rpki::publication::publication_object_elt](#).

Inherited by [irbe_cli.certificate_elt](#).

Static Public Attributes

- string [element_name](#) = "certificate"
- [payload_type](#) = [rpki.x509.X509](#)

10.124.1 Detailed Description

<certificate/> element.

Definition at line 278 of file publication.py.

10.124.2 Member Data Documentation

10.124.2.1 string rpki.publication.certificate_elt.element_name = "certificate" [static]

Definition at line 283 of file publication.py.

10.124.2.2 rpki.publication.certificate_elt.payload_type = rpki.x509.X509 [static]

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

Definition at line 284 of file publication.py.

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

- [publication.py \(2798\)](#)

10.125 rpki.publication.client_elt Class Reference

Inherits [rpki::publication::control_elt](#).

Inherited by [irbe_cli.client_elt](#).

Public Member Functions

- def [check_allowed_uri](#)
- def [endElement](#)
- def [serve_fetch_all](#)
- def [serve_fetch_one_maybe](#)
- def [serve_post_save_hook](#)

Static Public Attributes

- tuple [attributes](#) = ("action", "tag", "client_handle", "[base_uri](#)")
XML attributes for this element.
- [base_uri](#) = None
- [bpki_cert](#) = None
- [bpki_glue](#) = None
- [clear_https_ta_cache](#) = False
- string [element_name](#) = "client"
- tuple [elements](#) = ("bpki_cert", "[bpki_glue](#)")
XML elements contained by this element.
- tuple [sql_template](#) = [rpki.sql.template](#)("client", "client_id", "client_handle", "[base_uri](#)", ("bpki_cert", [rpki.x509.X509](#)), ("bpki_glue", [rpki.x509.X509](#)))

10.125.1 Detailed Description

<client/> element.

Definition at line 113 of file publication.py.

10.125.2 Member Function Documentation

10.125.2.1 def rpki.publication.client_elt.check_allowed_uri (self, uri)

Definition at line 160 of file publication.py.

10.125.2.2 def rpki.publication.client_elt.endElement (self, stack, name, text)

Handle subelements of <client/> element. These require special handling because modifying them invalidates the HTTPS trust anchor cache.

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

Definition at line 130 of file publication.py.

10.125.2.3 def rpki.publication.client_elt.serve_fetch_all (self)

Find client objects on which a list method should operate.

Definition at line 156 of file publication.py.

10.125.2.4 def rpki.publication.client_elt.serve_fetch_one_maybe (self)

Find the client object on which a get, set, or destroy method should operate, or which would conflict with a create method.

Definition at line 149 of file publication.py.

10.125.2.5 def rpki.publication.client_elt.serve_post_save_hook (self, q_pdu, r_pdu, cb, eb)

Extra server actions for client_elt.

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

Definition at line 140 of file publication.py.

10.125.3 Member Data Documentation

10.125.3.1 `tuple rpki.publication.client_elt.attributes = ("action", "tag", "client_handle", "base_uri") [static]`

XML attributes for this element.

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

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

10.125.3.2 `rpki.publication.client_elt.base_uri = None [static]`

Definition at line 124 of file `publication.py`.

10.125.3.3 `rpki.publication.client_elt.bpki_cert = None [static]`

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

10.125.3.4 `rpki.publication.client_elt.bpki_glue = None [static]`

Definition at line 126 of file `publication.py`.

10.125.3.5 `rpki.publication.client_elt.clear_https_ta_cache = False [static]`

Definition at line 128 of file `publication.py`.

10.125.3.6 `string rpki.publication.client_elt.element_name = "client" [static]`

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

10.125.3.7 tuple rpki.publication.client_elt.elements = ("bpki_cert",
"bpki_glue") [static]

XML elements contained by this element.

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

Definition at line 120 of file publication.py.

10.125.3.8 tuple rpki.publication.client_elt.sql_template =
rpki.sql.template("client", "client_id", "client_handle", "base_uri",
("bpki_cert", rpki.x509.X509), ("bpki_glue", rpki.x509.X509))
[static]

Definition at line 122 of file publication.py.

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

- [publication.py \(2798\)](#)

10.126 rpki.publication.cms_msg Class Reference

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

Inherited by [irbe_cli.publication cms_msg](#).

Static Public Attributes

- string [encoding](#) = "us-ascii"
- [saxify](#) = sax_handler.saxify
- [schema](#) = [rpki.relaxng.publication](#)

10.126.1 Detailed Description

Class to hold a CMS-signed publication PDU.

Definition at line 396 of file publication.py.

10.126.2 Member Data Documentation

10.126.2.1 `string rpki.publication.cms_msg.encoding = "us-ascii"` `[static]`

Definition at line 401 of file `publication.py`.

10.126.2.2 `rpki.publication.cms_msg.saxify = sax_handler.saxify` `[static]`

Reimplemented in [irbe_cli.publication_cms_msg](#).

Definition at line 403 of file `publication.py`.

10.126.2.3 `rpki.publication.cms_msg.schema = rpki.relaxng.publication` `[static]`

Definition at line 402 of file `publication.py`.

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

- [publication.py \(2798\)](#)

10.127 `rpki.publication.config_elt` Class Reference

Inherits [rpki::publication::control_elt](#).

Inherited by [irbe_cli.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

10.127.1 Detailed Description

<config/> element. This is a little weird because there should never be more than one row in the SQL config table, but we have to put the BPKI CRL somewhere and SQL is the least bad place available.

So we reuse a lot of the SQL machinery, but we nail `config_id` at 1, we don't expose it in the XML protocol, and we only support the get and set actions.

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

10.127.2 Member Function Documentation

10.127.2.1 `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`.

10.127.2.2 `def rpki.publication.config_elt.serve_fetch_one_maybe (self)`

Find the config object on which a get or set method should operate.

Definition at line 106 of file `publication.py`.

10.127.2.3 def rpki.publication.config_elt.serve_set (self, r_msg, cb, eb)

Handle a set action. This requires special handling because config doesn't support the create method.

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

Definition at line 96 of file publication.py.

10.127.2.4 def rpki.publication.config_elt.startElement (self, stack, name, attrs)

StartElement() handler for config object. This requires special handling because of the weird way we treat config_id.

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

Definition at line 80 of file publication.py.

10.127.3 Member Data Documentation**10.127.3.1 tuple rpki.publication.config_elt.attributes = ("action", "tag")
[static]**

XML attributes for this element.

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

Definition at line 72 of file publication.py.

10.127.3.2 rpki.publication.config_elt.config_id

Definition at line 86 of file publication.py.

**10.127.3.3 string rpki.publication.config_elt.element_name = "config"
[static]**

Definition at line 73 of file publication.py.

10.127.3.4 `tuple rpki.publication.config_elt.elements = ("bpki_crl",)`
[static]

XML elements contained by this element.

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

Definition at line 74 of file `publication.py`.

10.127.3.5 `tuple rpki.publication.config_elt.sql_template =`
`rpki.sql.template("config", "config_id", ("bpki_crl",`
`rpki.x509.CRL))` [static]

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

10.127.3.6 `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 \(2798\)](#)

10.128 rpki.publication.control_elt Class Reference

Inherits [rpki::xml_utils::data_elt](#), [rpki::sql::sql_persistent](#), and [rpki::publication::publication_namespace](#).

Inherited by [rpki.publication.client_elt](#), and [rpki.publication.config_elt](#).

Public Member Functions

- `def` [serve_dispatch](#)

10.128.1 Detailed Description

Virtual class for control channel objects.

Definition at line 47 of file `publication.py`.

10.128.2 Member Function Documentation

10.128.2.1 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 \(2798\)](#)

10.129 rpki.publication.crl_elt Class Reference

Inherits [rpki::publication::publication_object_elt](#).

Inherited by [irbe_cli.crl_elt](#).

Static Public Attributes

- string [element_name](#) = "crl"
- [payload_type](#) = [rpki.x509.CRL](#)

10.129.1 Detailed Description

<crl/> element.

Definition at line 286 of file publication.py.

10.129.2 Member Data Documentation

10.129.2.1 string rpki.publication.crl_elt.element_name = "crl" [static]

Definition at line 291 of file publication.py.

10.129.2.2 rpki.publication.crl_elt.payload_type = rpki.x509.CRL [static]

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

Definition at line 292 of file publication.py.

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

- [publication.py \(2798\)](#)

10.130 rpki.publication.manifest_elt Class Reference

Inherits [rpki::publication::publication_object_elt](#).

Inherited by [irbe_cli.manifest_elt](#).

Static Public Attributes

- string [element_name](#) = "manifest"
- [payload_type](#) = [rpki.x509.SignedManifest](#)

10.130.1 Detailed Description

```
<manifest/> element.
```

Definition at line 294 of file publication.py.

10.130.2 Member Data Documentation

10.130.2.1 string rpki.publication.manifest_elt.element_name = "manifest" [static]

Definition at line 299 of file publication.py.

10.130.2.2 rpki.publication.manifest_elt.payload_type = rpki.x509.SignedManifest [static]

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

Definition at line 300 of file publication.py.

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

- [publication.py \(2798\)](#)

10.131 rpki.publication.msg Class Reference

Inherits [rpki::xml_utils::msg](#), and [rpki::publication::publication_namespace](#).

Inherited by [irbe_cli.publication_msg](#).

Public Member Functions

- def [serve_top_level](#)

Static Public Attributes

- tuple [pdus](#)
Dispatch table of PDUs for this protocol.
- int [version](#) = 1
Protocol version.

10.131.1 Detailed Description

Publication PDU.

Definition at line 343 of file publication.py.

10.131.2 Member Function Documentation

10.131.2.1 def rpki.publication.msg.serve_top_level (self, gctx, client, cb)

Serve one msg PDU.

Definition at line 357 of file publication.py.

10.131.3 Member Data Documentation

10.131.3.1 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, roa_elt, report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented in [irbe_cli.publication_msg](#).

Definition at line 354 of file publication.py.

10.131.3.2 rpki::publication.msg::version = 1 [static]

Protocol version.

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

Definition at line 350 of file publication.py.

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

- [publication.py \(2798\)](#)

10.132 rpki.publication.publication_namespace Class Reference

Inherits [object](#).

Inherited by [rpki.publication.control_elt](#), [rpki.publication.msg](#), [rpki.publication.publication_object_elt](#), and [rpki.publication.report_error_elt](#).

Static Public Attributes

- dictionary [nsmap](#) = { None : [xmlns](#) }
- string [xmlns](#) = "http://www.hactrn.net/uris/rpki/publication-spec/"

10.132.1 Detailed Description

XML namespace parameters for publication protocol.

Definition at line 39 of file publication.py.

10.132.2 Member Data Documentation

10.132.2.1 dictionary `rpki.publication.publication_namespace.nsmap` = { `None` : `xmlns` } `[static]`

Definition at line 45 of file publication.py.

10.132.2.2 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 \(2798\)](#)

10.133 rpki.publication.publication_object_elt Class Reference

Inherits [rpki::xml_utils::base_elt](#), and [rpki::publication::publication_namespace](#).

Inherited by [rpki.publication.certificate_elt](#), [rpki.publication.crl_elt](#), [rpki.publication.manifest_elt](#), and [rpki.publication.roa_elt](#).

Public Member Functions

- def [endElement](#)
- def [make_publish](#)
- def [make_withdraw](#)
- def [serve_dispatch](#)
- def [serve_publish](#)
- def [serve_withdraw](#)
- def [toXML](#)
- def [uri_to_filename](#)

Static Public Attributes

- tuple [attributes](#) = ("action", "tag", "client_handle", "uri")

XML attributes for this element.

- `payload` = None
- `payload_type` = None

10.133.1 Detailed Description

Virtual class for publishable objects. These have very similar syntax, differences lie in underlying datatype and methods. XML methods are a little different from the pattern used for objects that support the create/set/get/list/destroy actions, but publishable objects don't go in SQL either so these classes would be different in any case.

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

10.133.2 Member Function Documentation

10.133.2.1 `def rpki.publication.publication_object_elt.endElement (self, stack, name, text)`

Handle a publishable element element.

Reimplemented from `rpki.xml_utils.base_elt`.

Definition at line 178 of file `publication.py`.

10.133.2.2 `def rpki.publication.publication_object_elt.make_publish (cls, uri, obj, tag = None)`

Construct a publication PDU.

Definition at line 257 of file `publication.py`.

10.133.2.3 `def rpki.publication.publication_object_elt.make_withdraw (cls, uri, obj, tag = None)`

Construct a withdrawal PDU.

Definition at line 268 of file `publication.py`.

10.133.2.4 `def rpki.publication.publication_object_elt.serve_dispatch (self, r_msg, cb, eb)`

Action dispatch handler.

Definition at line 196 of file publication.py.

10.133.2.5 `def rpki.publication.publication_object_elt.serve_publish (self)`

Publish an object.

Definition at line 215 of file publication.py.

10.133.2.6 `def rpki.publication.publication_object_elt.serve_withdraw (self)`

Withdraw an object.

Definition at line 228 of file publication.py.

10.133.2.7 `def rpki.publication.publication_object_elt.toXML (self)`

Generate XML element for publishable object.

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

Definition at line 187 of file publication.py.

10.133.2.8 `def rpki.publication.publication_object_elt.uri_to_filename (self)`

Convert a URI to a local filename.

Definition at line 242 of file publication.py.

10.133.3 Member Data Documentation

10.133.3.1 `tuple rpki.publication.publication_object_elt.attributes = ("action", "tag", "client_handle", "uri") [static]`

XML attributes for this element.

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

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

10.133.3.2 `rpki.publication.publication_object_elt.payload = None [static]`

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

10.133.3.3 `rpki.publication.publication_object_elt.payload_type = None [static]`

Reimplemented in [rpki.publication.certificate_elt](#), [rpki.publication.crl_elt](#), [rpki.publication.manifest_elt](#), and [rpki.publication.roa_elt](#).

Definition at line 175 of file `publication.py`.

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

- [publication.py \(2798\)](#)

10.134 `rpki.publication.report_error_elt` Class Reference

Inherits [rpki.xml_utils::text_elt](#), and [rpki::publication::publication_namespace](#).

Inherited by [irbe_cli.report_error_elt](#).

Public Member Functions

- `def __str__`
- `def from_exception`

Public Attributes

- `error_code`

- [tag](#)

Static Public Attributes

- tuple [attributes](#) = ("tag", "[error_code](#)")
XML attributes for this element.
- string [element_name](#) = "report_error"
- [error_text](#) = None
- string [text_attribute](#) = "error_text"
Name of the class attribute that holds the text value.

10.134.1 Detailed Description

`<report_error/>` element.

Definition at line 312 of file `publication.py`.

10.134.2 Member Function Documentation

10.134.2.1 `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 334 of file `publication.py`.

10.134.2.2 `def rpki.publication.report_error_elt.from_exception (cls, e, tag = None)`

Generate a `<report_error/>` element from an exception.

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

10.134.3 Member Data Documentation

10.134.3.1 `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 318 of file `publication.py`.

10.134.3.2 `string rpki.publication.report_error_elt.element_name = "report_error"` `[static]`

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

10.134.3.3 `rpki.publication.report_error_elt.error_code`

Definition at line 330 of file `publication.py`.

10.134.3.4 `rpki.publication.report_error_elt.error_text = None` `[static]`

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

10.134.3.5 `rpki.publication.report_error_elt.tag`

Definition at line 329 of file `publication.py`.

10.134.3.6 `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 319 of file publication.py.

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

- [publication.py \(2798\)](#)

10.135 rpki.publication.roa_elt Class Reference

Inherits [rpki::publication::publication_object_elt](#).

Inherited by [irbe_cli.roa_elt](#).

Static Public Attributes

- string [element_name](#) = "roa"
- [payload_type](#) = [rpki.x509.ROA](#)

10.135.1 Detailed Description

<roa/> element.

Definition at line 302 of file publication.py.

10.135.2 Member Data Documentation

10.135.2.1 string rpki.publication.roa_elt.element_name = "roa" [static]

Definition at line 307 of file publication.py.

10.135.2.2 rpki.publication.roa_elt.payload_type = rpki.x509.ROA [static]

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

Definition at line 308 of file publication.py.

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

- [publication.py \(2798\)](#)

10.136 rpki.publication.sax_handler Class Reference

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

Inherited by [irbe_cli.publication_sax_handler](#).

Static Public Attributes

- string [name](#) = "msg"
- [pdu](#) = [msg](#)
- string [version](#) = "1"

10.136.1 Detailed Description

SAX handler for publication protocol.

Definition at line 387 of file publication.py.

10.136.2 Member Data Documentation

10.136.2.1 string rpki.publication.sax_handler.name = "msg" [static]

Definition at line 393 of file publication.py.

10.136.2.2 rpki.publication.sax_handler.pdu = msg [static]

Reimplemented in [irbe_cli.publication_sax_handler](#).

Definition at line 392 of file publication.py.

10.136.2.3 string rpki.publication.sax_handler.version = "1" [static]

Definition at line 394 of file publication.py.

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

- [publication.py \(2798\)](#)

10.137 rpki.resource_set.resource_bag Class Reference

Inherits [object](#).

Public Member Functions

- def [__eq__](#)
- def [__init__](#)
- def [__ne__](#)
- def [__str__](#)
- def [empty](#)
- def [from_rfc3779_tuples](#)
- def [intersection](#)
- def [oversized](#)
- def [undersized](#)
- def [union](#)

Public Attributes

- [asn](#)
Set of Autonomous System Number resources.
- [v4](#)
Set of IPv4 resources.
- [v6](#)
Set of IPv6 resources.
- [valid_until](#)
Expiration date of resources, for setting certificate notAfter field.

10.137.1 Detailed Description

Container to simplify passing around the usual triple of ASN, IPv4, and IPv6 resource sets.

Definition at line 547 of file resource_set.py.

10.137.2 Member Function Documentation

10.137.2.1 `def rpki.resource_set.resource_bag.__eq__ (self, other)`

Definition at line 615 of file resource_set.py.

10.137.2.2 `def rpki.resource_set.resource_bag.__init__ (self, asn = None, v4 = None, v6 = None, valid_until = None)`

Definition at line 565 of file resource_set.py.

10.137.2.3 `def rpki.resource_set.resource_bag.__ne__ (self, other)`

Definition at line 621 of file resource_set.py.

10.137.2.4 `def rpki.resource_set.resource_bag.__str__ (self)`

Definition at line 644 of file resource_set.py.

10.137.2.5 `def rpki.resource_set.resource_bag.empty (self)`

True iff all resource sets in this bag are empty.

Definition at line 611 of file resource_set.py.

10.137.2.6 `def rpki.resource_set.resource_bag.from_rfc3779_tuples (cls, exts)`

Build a resource_bag from intermediate form generated by RFC 3779 ASN.1 decoder.

Definition at line 588 of file resource_set.py.

10.137.2.7 def rpki.resource_set.resource_bag.intersection (self, other)

Compute intersection with another resource_bag. valid_until attribute (if any) inherits from self.

Definition at line 624 of file resource_set.py.

10.137.2.8 def rpki.resource_set.resource_bag.oversized (self, other)

True iff self is oversized with respect to other.

Definition at line 571 of file resource_set.py.

10.137.2.9 def rpki.resource_set.resource_bag.undersized (self, other)

True iff self is undersized with respect to other.

Definition at line 579 of file resource_set.py.

10.137.2.10 def rpki.resource_set.resource_bag.union (self, other)

Compute union with another resource_bag. valid_until attribute (if any) inherits from self.

Definition at line 634 of file resource_set.py.

10.137.3 Member Data Documentation**10.137.3.1 rpki::resource_set.resource_bag::asn**

Set of Autonomous System Number resources.

Definition at line 566 of file resource_set.py.

10.137.3.2 rpki::resource_set.resource_bag::v4

Set of IPv4 resources.

Definition at line 567 of file resource_set.py.

10.137.3.3 rpki::resource_set.resource_bag::v6

Set of IPv6 resources.

Definition at line 568 of file resource_set.py.

10.137.3.4 rpki::resource_set.resource_bag::valid_until

Expiration date of resources, for setting certificate notAfter field.

Definition at line 569 of file resource_set.py.

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

- [resource_set.py \(2776\)](#)

10.138 rpki.resource_set.resource_range Class Reference

Inherits [object](#).

Inherited by [rpki.resource_set.resource_range_as](#), and [rpki.resource_set.resource_range_ip](#).

Public Member Functions

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

Public Attributes

- [max](#)
- [min](#)

10.138.1 Detailed Description

Generic resource range type. Assumes underlying type is some kind of integer.

This is a virtual class. You probably don't want to use this type directly.

Definition at line 50 of file resource_set.py.

10.138.2 Member Function Documentation

10.138.2.1 def rpki.resource_set.resource_range.__cmp__(self, other)

Compare two resource_range objects.

Definition at line 67 of file resource_set.py.

10.138.2.2 def rpki.resource_set.resource_range.__init__(self, min, max)

Initialize and sanity check a resource_range.

Definition at line 59 of file resource_set.py.

10.138.3 Member Data Documentation

10.138.3.1 rpki.resource_set.resource_range.max

Definition at line 65 of file resource_set.py.

10.138.3.2 rpki.resource_set.resource_range.min

Reimplemented in [rpki.resource_set.resource_range_as](#).

Definition at line 64 of file resource_set.py.

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

- [resource_set.py \(2776\)](#)

10.139 rpki.resource_set.resource_range_as Class Reference

Inherits [rpki::resource_set::resource_range](#).

Public Member Functions

- [def __str__](#)
- [def to_rfc3779_tuple](#)

Public Attributes

- [min](#)

Static Public Attributes

- [datum_type = long](#)
Type of underlying data (min and max).

10.139.1 Detailed Description

Range of Autonomous System Numbers.

Denotes a single ASN by a range whose min and max values are identical.

Definition at line 78 of file resource_set.py.

10.139.2 Member Function Documentation

10.139.2.1 `def rpki.resource_set.resource_range_as.__str__ (self)`

Convert a resource_range_as to string format.

Definition at line 91 of file resource_set.py.

10.139.2.2 `def rpki.resource_set.resource_range_as.to_rfc3779_tuple (self)`

Convert a `resource_range_as` to tuple format for RFC 3779 ASN.1 encoding.

Definition at line 100 of file `resource_set.py`.

10.139.3 Member Data Documentation

10.139.3.1 `rpki::resource_set.resource_range_as::datum_type = long` [static]

Type of underlying data (min and max).

Definition at line 89 of file `resource_set.py`.

10.139.3.2 `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 \(2776\)](#)

10.140 rpki.resource_set.resource_range_ip Class Reference

Inherits [rpki::resource_set::resource_range](#).

Inherited by [rpki.resource_set.resource_range_ipv4](#), and [rpki.resource_set.resource_range_ipv6](#).

Public Member Functions

- def [__str__](#)
- def [make_prefix](#)
- def [to_rfc3779_tuple](#)

Private Member Functions

- def [_prefixlen](#)

10.140.1 Detailed Description

Range of (generic) IP addresses.

Prefixes are converted to ranges on input, and ranges that can be represented as prefixes are written as prefixes on output.

This is a virtual class. You probably don't want to use it directly.

Definition at line 109 of file resource_set.py.

10.140.2 Member Function Documentation

10.140.2.1 def rpki.resource_set.resource_range_ip.__str__ (self)

Convert a resource_range_ip to string format.

Definition at line 137 of file resource_set.py.

10.140.2.2 def rpki.resource_set.resource_range_ip._prefixlen (self) [private]

Determine whether a resource_range_ip can be expressed as a prefix.

Definition at line 120 of file resource_set.py.

10.140.2.3 def rpki.resource_set.resource_range_ip.make_prefix (cls, prefix, prefixlen)

Construct a resource range corresponding to a prefix.

Definition at line 160 of file resource_set.py.

10.140.2.4 def rpki.resource_set.resource_range_ip.to_rfc3779_tuple (self)

Convert a resource_range_ip to tuple format for RFC 3779 ASN.1 encoding.

Definition at line 147 of file resource_set.py.

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

- [resource_set.py \(2776\)](#)

10.141 rpki.resource_set.resource_range_ipv4 Class Reference

Inherits [rpki::resource_set::resource_range_ip](#).

Static Public Attributes

- [datum_type = rpki.ipaddrs.v4addr](#)
Type of underlying data (min and max).

10.141.1 Detailed Description

Range of IPv4 addresses.

Definition at line 170 of file resource_set.py.

10.141.2 Member Data Documentation

10.141.2.1 rpki::resource_set.resource_range_ipv4::datum_type = rpki.ipaddrs.v4addr [static]

Type of underlying data (min and max).

Definition at line 178 of file resource_set.py.

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

- [resource_set.py \(2776\)](#)

10.142 `rpki.resource_set.resource_range_ipv6` Class Reference

Inherits [rpki::resource_set::resource_range_ip](#).

Static Public Attributes

- `datum_type = rpki.ipaddrs.v6addr`
Type of underlying data (min and max).

10.142.1 Detailed Description

Range of IPv6 addresses.

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

10.142.2 Member Data Documentation

10.142.2.1 `rpki::resource_set.resource_range_ipv6::datum_type = rpki.ipaddrs.v6addr` [static]

Type of underlying data (min and max).

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

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

- [resource_set.py \(2776\)](#)

10.143 `rpki.resource_set.resource_set` Class Reference

Inherits `list`.

Inherited by [rpki.resource_set.resource_set_as](#), and [rpki.resource_set.resource_set_ip](#).

Public Member Functions

- `def __init__`
- `def __str__`
- `def contains`
- `def difference`
- `def from_sql`

- def [intersection](#)
- def [issubset](#)
- def [issuperset](#)
- def [symmetric_difference](#)
- def [union](#)

Static Public Attributes

- [inherit](#) = False
Boolean indicating whether this [resource_set](#) uses RFC 3779 inheritance.

Private Member Functions

- def [_comm](#)

10.143.1 Detailed Description

Generic resource set, a list subclass containing resource ranges.

This is a virtual class. You probably don't want to use it directly.

Definition at line 206 of file resource_set.py.

10.143.2 Member Function Documentation

10.143.2.1 def rpki.resource_set.resource_set.__init__ (self, ini = None)

Initialize a resource_set.

Definition at line 219 of file resource_set.py.

10.143.2.2 def rpki.resource_set.resource_set.__str__ (self)

Convert a resource_set to string format.

Definition at line 246 of file resource_set.py.

10.143.2.3 `def rpki.resource_set.resource_set.comm (self, other)` `[private]`

Like `comm(1)`, sort of.

Returns a tuple of three resource sets: resources only in `self`, resources only in `other`, and resources in both. Used (not very efficiently) as the basis for most set operations on resource sets.

Definition at line 255 of file `resource_set.py`.

10.143.2.4 `def rpki.resource_set.resource_set.contains (self, item)`

Set membership test for resource sets.

Definition at line 332 of file `resource_set.py`.

10.143.2.5 `def rpki.resource_set.resource_set.difference (self, other)`

Set difference for resource sets.

Definition at line 323 of file `resource_set.py`.

10.143.2.6 `def rpki.resource_set.resource_set.from_sql (cls, sql, query, args = None)`

Create resource set from an SQL query.

`sql` is an object that supports `execute()` and `fetchall()` methods like a DB API 2.0 cursor object.

`query` is an SQL query that returns a sequence of (min, max) pairs.

Definition at line 369 of file `resource_set.py`.

10.143.2.7 def rpki.resource_set.resource_set.intersection (*self*, *other*)

Set intersection for resource sets.

Definition at line 319 of file resource_set.py.

10.143.2.8 def rpki.resource_set.resource_set.issubset (*self*, *other*)

Test whether self is a subset (possibly improper) of other.

Definition at line 355 of file resource_set.py.

10.143.2.9 def rpki.resource_set.resource_set.issuperset (*self*, *other*)

Test whether self is a superset (possibly improper) of other.

Definition at line 364 of file resource_set.py.

**10.143.2.10 def rpki.resource_set.resource_set.symmetric_difference (*self*,
other)**

Set symmetric difference (XOR) for resource sets.

Definition at line 327 of file resource_set.py.

10.143.2.11 def rpki.resource_set.resource_set.union (*self*, *other*)

Set union for resource sets.

Definition at line 288 of file resource_set.py.

10.143.3 Member Data Documentation

10.143.3.1 rpki::resource_set.resource_set::inherit = False [static]

Boolean indicating whether this [resource_set](#) uses RFC 3779 inheritance.

Reimplemented in [rpki.resource_set.resource_set_as](#), and [rpki.resource_set.resource_set_ip](#).

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

The documentation for this class was generated from the following file:

- [resource_set.py \(2776\)](#)

10.144 rpki.resource_set.resource_set_as Class Reference

Inherits [rpki::resource_set::resource_set](#).

Public Member Functions

- def [parse_rfc3779_tuple](#)
- def [parse_str](#)
- def [to_rfc3779_tuple](#)

Public Attributes

- [inherit](#)

Boolean indicating whether this [resource_set](#) uses RFC 3779 inheritance.

Static Public Attributes

- [range_type](#) = [resource_range_as](#)

Type of range underlying this type of [resource_set](#).

10.144.1 Detailed Description

Autonomous System Number resource set.

Definition at line 384 of file `resource_set.py`.

10.144.2 Member Function Documentation

10.144.2.1 `def rpki.resource_set.resource_set_as.parse_rfc3779_tuple (self, x)`

Parse ASN resource from tuple format generated by RFC 3779 ASN.1 decoder.

Definition at line 404 of file resource_set.py.

10.144.2.2 `def rpki.resource_set.resource_set_as.parse_str (self, x)`

Parse ASN resource sets from text (eg, XML attributes).

Definition at line 394 of file resource_set.py.

10.144.2.3 `def rpki.resource_set.resource_set_as.to_rfc3779_tuple (self)`

Convert ASN resource set into tuple format used for RFC 3779 ASN.1 encoding.

Definition at line 422 of file resource_set.py.

10.144.3 Member Data Documentation

10.144.3.1 `rpki.resource_set.resource_set_as.inherit`

Boolean indicating whether this [resource_set](#) uses RFC 3779 inheritance.

Reimplemented from [rpki.resource_set.resource_set](#).

Definition at line 420 of file resource_set.py.

10.144.3.2 `rpki::resource_set.resource_set_as::range_type = resource_range_as` `[static]`

Type of range underlying this type of [resource_set](#).

Definition at line 392 of file resource_set.py.

The documentation for this class was generated from the following file:

- [resource_set.py \(2776\)](#)

10.145 rpki.resource_set.resource_set_ip Class Reference

Inherits [rpki::resource_set::resource_set](#).

Inherited by [rpki.resource_set.resource_set_ipv4](#), and [rpki.resource_set.resource_set_ipv6](#).

Public Member Functions

- def [parse_rfc3779_tuple](#)
- def [parse_str](#)
- def [to_rfc3779_tuple](#)

Public Attributes

- [inherit](#)
Boolean indicating whether this [resource_set](#) uses RFC 3779 inheritance.

10.145.1 Detailed Description

(Generic) IP address resource set.

This is a virtual class. You probably don't want to use it directly.

Definition at line 434 of file resource_set.py.

10.145.2 Member Function Documentation

10.145.2.1 def rpki.resource_set.resource_set_ip.parse_rfc3779_tuple (self, x)

Parse IP address resource sets from tuple format generated by RFC 3779 ASN.1 decoder.

Definition at line 454 of file resource_set.py.

10.145.2.2 def rpki.resource_set.resource_set_ip.parse_str (self, x)

Parse IP address resource sets from text (eg, XML attributes).

Definition at line 442 of file resource_set.py.

10.145.2.3 def rpki.resource_set.resource_set_ip.to_rfc3779_tuple (self)

Convert IP resource set into tuple format used by RFC 3779 ASN.1 encoder.

Definition at line 472 of file resource_set.py.

10.145.3 Member Data Documentation

10.145.3.1 rpki.resource_set.resource_set_ip.inherit

Boolean indicating whether this [resource_set](#) uses RFC 3779 inheritance.

Reimplemented from [rpki.resource_set.resource_set](#).

Definition at line 470 of file resource_set.py.

The documentation for this class was generated from the following file:

- [resource_set.py \(2776\)](#)

10.146 rpki.resource_set.resource_set_ipv4 Class Reference

Inherits [rpki::resource_set::resource_set_ip](#).

Static Public Attributes

- string [afi](#) = "\x00\x01"
Address Family Identifier value for IPv4.
- [range_type](#) = [resource_range_ipv4](#)
Type of range underlying this type of [resource_set](#).

10.146.1 Detailed Description

IPv4 address resource set.

Definition at line 484 of file resource_set.py.

10.146.2 Member Data Documentation

10.146.2.1 rpki::resource_set.resource_set_ipv4::afi = "\x00\x01" [static]

Address Family Identifier value for IPv4.

Definition at line 497 of file resource_set.py.

10.146.2.2 rpki::resource_set.resource_set_ipv4::range_type = resource_range_ipv4 [static]

Type of range underlying this type of [resource_set](#).

Definition at line 492 of file resource_set.py.

The documentation for this class was generated from the following file:

- [resource_set.py \(2776\)](#)

10.147 rpki.resource_set.resource_set_ipv6 Class Reference

Inherits [rpki::resource_set::resource_set_ip](#).

Static Public Attributes

- string [afi](#) = "\x00\x02"
Address Family Identifier value for IPv6.
- [range_type](#) = [resource_range_ipv6](#)
Type of range underlying this type of [resource_set](#).

10.147.1 Detailed Description

IPv6 address resource set.

Definition at line 499 of file resource_set.py.

10.147.2 Member Data Documentation

10.147.2.1 rpki::resource_set.resource_set_ipv6::afi = "\x00\x02" [static]

Address Family Identifier value for IPv6.

Definition at line 512 of file resource_set.py.

10.147.2.2 rpki::resource_set.resource_set_ipv6::range_type = resource_range_ipv6 [static]

Type of range underlying this type of [resource_set](#).

Definition at line 507 of file resource_set.py.

The documentation for this class was generated from the following file:

- [resource_set.py \(2776\)](#)

10.148 rpki.resource_set.roa_prefix Class Reference

Inherits [object](#).

Inherited by [rpki.resource_set.roa_prefix_ipv4](#), and [rpki.resource_set.roa_prefix_ipv6](#).

Public Member Functions

- def [__cmp__](#)
- def [__init__](#)
- def [__str__](#)
- def [max](#)
- def [min](#)
- def [to_resource_range](#)
- def [to_roa_tuple](#)

Public Attributes

- `max_prefixlen`
Maximum prefix length.
- `prefix`
The prefix itself, an IP address with bits beyond the prefix length zeroed.
- `prefixlen`
(Minimum) prefix length.

10.148.1 Detailed Description

ROA prefix. This is similar to the `resource_range_ip` class, but differs in that it only represents prefixes, never ranges, and includes the maximum prefix length as an additional value.

This is a virtual class, you probably don't want to use it directly.

Definition at line 666 of file `resource_set.py`.

10.148.2 Member Function Documentation

10.148.2.1 `def rpki.resource_set.roa_prefix.__cmp__(self, other)`

Compare two ROA prefix objects. Comparison is based on `prefix`, `prefixlen`, and `max_prefixlen`, in that order.

Definition at line 697 of file `resource_set.py`.

10.148.2.2 `def rpki.resource_set.roa_prefix.__init__(self, prefix, prefixlen, max_prefixlen = None)`

Initialize a ROA prefix. `max_prefixlen` is optional and defaults to `prefixlen`. `max_prefixlen` must not be smaller than `prefixlen`.

Definition at line 685 of file `resource_set.py`.

10.148.2.3 def rpki.resource_set.roa_prefix.__str__ (self)

Convert a ROA prefix to string format.

Definition at line 710 of file resource_set.py.

10.148.2.4 def rpki.resource_set.roa_prefix.max (self)

Return highest address covered by prefix.

Definition at line 731 of file resource_set.py.

10.148.2.5 def rpki.resource_set.roa_prefix.min (self)

Return lowest address covered by prefix.

Definition at line 727 of file resource_set.py.

10.148.2.6 def rpki.resource_set.roa_prefix.to_resource_range (self)

Convert this ROA prefix to the equivalent resource_range_ip object. This is an irreversable transformation because it loses the max_prefixlen attribute, nothing we can do about that.

Definition at line 719 of file resource_set.py.

10.148.2.7 def rpki.resource_set.roa_prefix.to_roa_tuple (self)

Convert a resource_range_ip to tuple format for ROA ASN.1 encoding.

Definition at line 738 of file resource_set.py.

10.148.3 Member Data Documentation

10.148.3.1 rpki::resource_set.roa_prefix::max_prefixlen

Maximum prefix length.

Definition at line 695 of file resource_set.py.

10.148.3.2 rpki::resource_set.roa_prefix::prefix

The prefix itself, an IP address with bits beyond the prefix length zeroed.

Definition at line 693 of file resource_set.py.

10.148.3.3 rpki::resource_set.roa_prefix::prefixlen

(Minimum) prefix length.

Definition at line 694 of file resource_set.py.

The documentation for this class was generated from the following file:

- [resource_set.py \(2776\)](#)

10.149 rpki.resource_set.roa_prefix_ipv4 Class Reference

Inherits [rpki::resource_set::roa_prefix](#).

Static Public Attributes

- [range_type = resource_range_ipv4](#)
Type of corresponding [resource_range_ip](#).

10.149.1 Detailed Description

IPv4 ROA prefix.

Definition at line 746 of file resource_set.py.

10.149.2 Member Data Documentation

10.149.2.1 `rpki::resource_set.roa_prefix_ipv4::range_type = resource_range_ipv4` `[static]`

Type of corresponding [resource_range_ip](#).

Definition at line 754 of file `resource_set.py`.

The documentation for this class was generated from the following file:

- [resource_set.py \(2776\)](#)

10.150 rpki.resource_set.roa_prefix_ipv6 Class Reference

Inherits [rpki::resource_set::roa_prefix](#).

Static Public Attributes

- `range_type = resource_range_ipv6`
Type of corresponding [resource_range_ip](#).

10.150.1 Detailed Description

IPv6 ROA prefix.

Definition at line 756 of file `resource_set.py`.

10.150.2 Member Data Documentation

10.150.2.1 `rpki::resource_set.roa_prefix_ipv6::range_type = resource_range_ipv6` `[static]`

Type of corresponding [resource_range_ip](#).

Definition at line 764 of file `resource_set.py`.

The documentation for this class was generated from the following file:

- [resource_set.py \(2776\)](#)

10.151 rpki.resource_set.roa_prefix_set Class Reference

Inherits list.

Inherited by [rpki.resource_set.roa_prefix_set_ipv4](#), and [rpki.resource_set.roa_prefix_set_ipv6](#).

Public Member Functions

- [def __init__](#)
- [def __str__](#)
- [def from_sql](#)
- [def parse_str](#)
- [def to_resource_set](#)
- [def to_roa_tuple](#)

10.151.1 Detailed Description

Set of ROA prefixes, analogous to the `resource_set_ip` class.

Definition at line 766 of file `resource_set.py`.

10.151.2 Member Function Documentation

10.151.2.1 `def rpki.resource_set.roa_prefix_set.__init__ (self, ini = None)`

Initialize a ROA prefix set.

Definition at line 771 of file `resource_set.py`.

10.151.2.2 `def rpki.resource_set.roa_prefix_set.__str__ (self)`

Convert a ROA prefix set to string format.

Definition at line 791 of file `resource_set.py`.

10.151.2.3 `def rpki.resource_set.roa_prefix_set.from_sql (cls, sql, query, args = None)`

Create ROA prefix set from an SQL query.

sql is an object that supports execute() and fetchall() methods like a DB API 2.0 cursor object.

query is an SQL query that returns a sequence of (prefix, prefixlen, max_prefixlen) triples.

Definition at line 825 of file resource_set.py.

10.151.2.4 `def rpki.resource_set.roa_prefix_set.parse_str (self, x)`

Parse ROA prefix from text (eg, an XML attribute).

Definition at line 795 of file resource_set.py.

10.151.2.5 `def rpki.resource_set.roa_prefix_set.to_resource_set (self)`

Convert a ROA prefix set to a resource set. This is an irreversable transformation. We have to compute a union here because ROA prefix sets can include overlaps, while RFC 3779 resource sets cannot. This is ugly, and there is almost certainly a more efficient way to do this, but start by getting the output right before worrying about making it fast or pretty.

Definition at line 807 of file resource_set.py.

10.151.2.6 `def rpki.resource_set.roa_prefix_set.to_roa_tuple (self)`

Convert ROA prefix set into tuple format used by ROA ASN.1 encoder. This is a variation on the format used in RFC 3779.

Definition at line 840 of file resource_set.py.

The documentation for this class was generated from the following file:

- [resource_set.py \(2776\)](#)

10.152 rpki.resource_set.roa_prefix_set_ipv4 Class Reference

Inherits [rpki::resource_set::roa_prefix_set](#).

Static Public Attributes

- [prefix_type](#) = [roa_prefix_ipv4](#)
Type of underlying [roa_prefix](#).
- [resource_set_type](#) = [resource_set_ipv4](#)
Type of corresponding [resource_set_ip](#) class.

10.152.1 Detailed Description

Set of IPv4 ROA prefixes.

Definition at line 850 of file [resource_set.py](#).

10.152.2 Member Data Documentation

10.152.2.1 rpki::resource_set.roa_prefix_set_ipv4::prefix_type = [roa_prefix_ipv4](#) [static]

Type of underlying [roa_prefix](#).

Definition at line 858 of file [resource_set.py](#).

10.152.2.2 rpki::resource_set.roa_prefix_set_ipv4::resource_set_type = [resource_set_ipv4](#) [static]

Type of corresponding [resource_set_ip](#) class.

Definition at line 863 of file [resource_set.py](#).

The documentation for this class was generated from the following file:

- [resource_set.py](#) (2776)

10.153 rpki.resource_set.roa_prefix_set_ipv6 Class Reference

Inherits [rpki::resource_set::roa_prefix_set](#).

Static Public Attributes

- [prefix_type](#) = [roa_prefix_ipv6](#)
Type of underlying [roa_prefix](#).
- [resource_set_type](#) = [resource_set_ipv6](#)
Type of corresponding [resource_set_ip](#) class.

10.153.1 Detailed Description

Set of IPv6 ROA prefixes.

Definition at line 865 of file [resource_set.py](#).

10.153.2 Member Data Documentation

10.153.2.1 [rpki::resource_set.roa_prefix_set_ipv6::prefix_type](#) = [roa_prefix_ipv6](#) [static]

Type of underlying [roa_prefix](#).

Definition at line 873 of file [resource_set.py](#).

10.153.2.2 [rpki::resource_set.roa_prefix_set_ipv6::resource_set_type](#) = [resource_set_ipv6](#) [static]

Type of corresponding [resource_set_ip](#) class.

Definition at line 878 of file [resource_set.py](#).

The documentation for this class was generated from the following file:

- [resource_set.py](#) (2776)

10.154 rpki.roa.ROAIPAddress Class Reference

Inherits [Sequence](#).

Public Member Functions

- [def __init__](#)

Public Attributes

- [address](#)
- [maxLength](#)

10.154.1 Detailed Description

Definition at line 47 of file roa.py.

10.154.2 Member Function Documentation

10.154.2.1 `def rpki.roa.ROAIPAddress.__init__ (self, optional = 0, default = '')`

Definition at line 48 of file roa.py.

10.154.3 Member Data Documentation

10.154.3.1 `rpki.roa.ROAIPAddress.address`

Definition at line 49 of file roa.py.

10.154.3.2 `rpki.roa.ROAIPAddress.maxLength`

Definition at line 50 of file roa.py.

The documentation for this class was generated from the following file:

- [roa.py \(2424\)](#)

10.155 rpki.roa.ROAIPAddresses Class Reference

Inherits [SequenceOf](#).

Public Member Functions

- [def __init__](#)

10.155.1 Detailed Description

Definition at line 54 of file roa.py.

10.155.2 Member Function Documentation

10.155.2.1 `def rpki.roa.ROAIPAddresses.__init__(self, optional = 0, default = "")`

Definition at line 55 of file roa.py.

The documentation for this class was generated from the following file:

- [roa.py \(2424\)](#)

10.156 rpki.roa.ROAIPAddressFamilies Class Reference

Inherits [SequenceOf](#).

Public Member Functions

- [def __init__](#)

10.156.1 Detailed Description

Definition at line 65 of file roa.py.

10.156.2 Member Function Documentation

10.156.2.1 `def rpki.roa.ROAIPAddressFamilies.__init__ (self, optional = 0, default = '')`

Definition at line 66 of file roa.py.

The documentation for this class was generated from the following file:

- [roa.py \(2424\)](#)

10.157 rpki.roa.ROAIPAddressFamily Class Reference

Inherits [Sequence](#).

Public Member Functions

- `def __init__`

Public Attributes

- [addresses](#)
- [addressFamily](#)

10.157.1 Detailed Description

Definition at line 58 of file roa.py.

10.157.2 Member Function Documentation

10.157.2.1 `def rpki.roa.ROAIPAddressFamily.__init__ (self, optional = 0, default = '')`

Definition at line 59 of file roa.py.

10.157.3 Member Data Documentation

10.157.3.1 rpki.roa.ROAIPAddressFamily.addresses

Definition at line 61 of file roa.py.

10.157.3.2 rpki.roa.ROAIPAddressFamily.addressFamily

Definition at line 60 of file roa.py.

The documentation for this class was generated from the following file:

- [roa.py \(2424\)](#)

10.158 rpki.roa.RouteOriginAttestation Class Reference

Inherits [Sequence](#).

Public Member Functions

- `def __init__`

Public Attributes

- [asID](#)
- [explicitVersion](#)
- [ipAddrBlocks](#)
- [version](#)

10.158.1 Detailed Description

Definition at line 69 of file roa.py.

10.158.2 Member Function Documentation

- 10.158.2.1** `def rpki.roa.RouteOriginAttestation.__init__ (self, optional = 0, default = '')`

Definition at line 70 of file roa.py.

10.158.3 Member Data Documentation

10.158.3.1 rpki.roa.RouteOriginAttestation.asID

Definition at line 73 of file roa.py.

10.158.3.2 rpki.roa.RouteOriginAttestation.explicitVersion

Definition at line 72 of file roa.py.

10.158.3.3 rpki.roa.RouteOriginAttestation.ipAddrBlocks

Definition at line 74 of file roa.py.

10.158.3.4 rpki.roa.RouteOriginAttestation.version

Definition at line 71 of file roa.py.

The documentation for this class was generated from the following file:

- [roa.py \(2424\)](#)

10.159 rpki.rpki_engine.ca_detail_obj Class Reference

Inherits [rpki::sql::sql_persistent](#).

Public Member Functions

- def [activate](#)
- def [ca](#)
- def [child_certs](#)
- def [create](#)
- def [crl_uri](#)

- def [crl_uri_tail](#)
- def [delete](#)
- def [generate_crl](#)
- def [generate_manifest](#)
- def [generate_manifest_cert](#)
- def [issue](#)
- def [issue_ee](#)
- def [manifest_uri](#)
- def [revoke](#)
- def [revoked_certs](#)
- def [roas](#)
- def [sql_decode](#)
- def [update](#)

Public Attributes

- [ca_cert_uri](#)
- [ca_id](#)
- [gctx](#)
- [latest_ca_cert](#)
- [latest_crl](#)
- [latest_manifest](#)
- [latest_manifest_cert](#)
- [manifest_private_key_id](#)
- [manifest_public_key](#)
- [nextUpdate](#)
- [private_key_id](#)
- [public_key](#)
- [state](#)

Static Public Attributes

- tuple [sql_template](#)

10.159.1 Detailed Description

Internal CA detail object.

Definition at line 541 of file rpki_engine.py.

10.159.2 Member Function Documentation

10.159.2.1 `def rpki.rpki_engine.ca_detail_obj.activate (self, ca, cert, uri, callback, errback, predecessor = None)`

Activate this ca_detail.

Definition at line 597 of file rpki_engine.py.

10.159.2.2 `def rpki.rpki_engine.ca_detail_obj.ca (self)`

Fetch CA object to which this ca_detail links.

Definition at line 569 of file rpki_engine.py.

10.159.2.3 `def rpki.rpki_engine.ca_detail_obj.child_certs (self, child = None, ski = None, unique = False)`

Fetch all child_cert objects that link to this ca_detail.

Definition at line 573 of file rpki_engine.py.

10.159.2.4 `def rpki.rpki_engine.ca_detail_obj.create (cls, ca)`

Create a new ca_detail object for a specified CA.

Definition at line 754 of file rpki_engine.py.

10.159.2.5 `def rpki.rpki_engine.ca_detail_obj.crl_uri (self, ca)`

Return publication URI for this ca_detail's CRL.

Definition at line 585 of file rpki_engine.py.

10.159.2.6 `def rpki.rpki_engine.ca_detail_obj.crl_uri_tail (self)`

Return tail (filename portion) of publication URI for this ca_detail's CRL.

Definition at line 589 of file rpki_engine.py.

10.159.2.7 `def rpki.rpki_engine.ca_detail_obj.delete (self, ca, repository, cb, eb, 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 630 of file rpki_engine.py.

10.159.2.8 `def rpki.rpki_engine.ca_detail_obj.generate_crl (self, callback, errback, 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 845 of file rpki_engine.py.

10.159.2.9 `def rpki.rpki_engine.ca_detail_obj.generate_manifest (self, callback, errback, nextUpdate = None)`

Generate a new manifest for this ca_detail.

Definition at line 879 of file rpki_engine.py.

10.159.2.10 `def rpki.rpki_engine.ca_detail_obj.generate_manifest_cert (self, ca)`

Generate a new manifest certificate for this ca_detail.

Definition at line 789 of file rpki_engine.py.

10.159.2.11 `def rpki.rpki_engine.ca_detail_obj.issue (self, ca, child, subject_key, sia, resources, callback, errback, 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 801 of file rpki_engine.py.

10.159.2.12 `def rpki.rpki_engine.ca_detail_obj.issue_ee (self, ca, resources, subject_key, sia = None)`

Issue a new EE certificate.

Definition at line 772 of file rpki_engine.py.

10.159.2.13 `def rpki.rpki_engine.ca_detail_obj.manifest_uri (self, ca)`

Return publication URI for this ca_detail's manifest.

Definition at line 593 of file rpki_engine.py.

10.159.2.14 `def rpki.rpki_engine.ca_detail_obj.revoke (self, cb, eb)`

Request revocation of all certificates whose SKI matches the key for this ca_detail.

Tasks:

- Request revocation of old keypair by parent.
- Revoke all child certs issued by the old keypair.
- Generate a final CRL, signed with the old keypair, listing all the revoked certs, with a next CRL time after the last cert or CRL signed by the old keypair will have expired.
- Generate a corresponding final manifest.
- Destroy old keypairs.
- Leave final CRL and manifest in place until their nextupdate time has passed.

Definition at line 661 of file rpki_engine.py.

10.159.2.15 def rpki.rpki_engine.ca_detail_obj.revoked_certs (self)

Fetch all revoked_cert objects that link to this ca_detail.

Definition at line 577 of file rpki_engine.py.

10.159.2.16 def rpki.rpki_engine.ca_detail_obj.roas (self)

Fetch all ROA objects that link to this ca_detail.

Definition at line 581 of file rpki_engine.py.

10.159.2.17 def rpki.rpki_engine.ca_detail_obj.sql_decode (self, vals)

Extra assertions for SQL decode of a ca_detail_obj.

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 561 of file rpki_engine.py.

10.159.2.18 `def rpki.rpki_engine.ca_detail_obj.update (self, parent, ca, rc, sia_uri_changed, old_resources, callback, errback)`

Need to get a new certificate for this ca_detail and perhaps frob children of this ca_detail.

Definition at line 725 of file rpki_engine.py.

10.159.3 Member Data Documentation**10.159.3.1** `rpki.rpki_engine.ca_detail_obj.ca_cert_uri`

Definition at line 603 of file rpki_engine.py.

10.159.3.2 `rpki.rpki_engine.ca_detail_obj.ca_id`

Definition at line 760 of file rpki_engine.py.

10.159.3.3 `rpki.rpki_engine.ca_detail_obj.gctx`

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 759 of file rpki_engine.py.

10.159.3.4 `rpki.rpki_engine.ca_detail_obj.latest_ca_cert`

Definition at line 602 of file rpki_engine.py.

10.159.3.5 `rpki.rpki_engine.ca_detail_obj.latest_crl`

Definition at line 869 of file rpki_engine.py.

10.159.3.6 rpki.rpki_engine.ca_detail_obj.latest_manifest

Definition at line 900 of file rpki_engine.py.

10.159.3.7 rpki.rpki_engine.ca_detail_obj.latest_manifest_cert

Definition at line 716 of file rpki_engine.py.

10.159.3.8 rpki.rpki_engine.ca_detail_obj.manifest_private_key_id

Definition at line 714 of file rpki_engine.py.

10.159.3.9 rpki.rpki_engine.ca_detail_obj.manifest_public_key

Definition at line 715 of file rpki_engine.py.

10.159.3.10 rpki.rpki_engine.ca_detail_obj.nextUpdate

Definition at line 693 of file rpki_engine.py.

10.159.3.11 rpki.rpki_engine.ca_detail_obj.private_key_id

Definition at line 713 of file rpki_engine.py.

10.159.3.12 rpki.rpki_engine.ca_detail_obj.public_key

Definition at line 764 of file rpki_engine.py.

10.159.3.13 tuple rpki.rpki_engine.ca_detail_obj.sql_template [static]

Initial value:

```
rpki.sql.template(  
    "ca_detail",  
    "ca_detail_id",  
    ("private_key_id",          rpki.x509.RSA),  
    ("public_key",              rpki.x509.RSAPublic),  
    ("latest_ca_cert",          rpki.x509.X509),  
    ("manifest_private_key_id", rpki.x509.RSA),  
    ("manifest_public_key",     rpki.x509.RSAPublic),  
    ("latest_manifest_cert",    rpki.x509.X509),  
    ("latest_manifest",         rpki.x509.SignedManifest),  
    ("latest_crl",              rpki.x509.CRL),  
    "state",  
    "ca_cert_uri",  
    "ca_id")
```

Definition at line 546 of file rpki_engine.py.

10.159.3.14 rpki.rpki_engine.ca_detail_obj.state

Definition at line 610 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- [rpki_engine.py \(2793\)](#)

10.160 rpki.rpki_engine.ca_obj Class Reference

Inherits [rpki::sql::sql_persistent](#).

Public Member Functions

- def [ca_details](#)
- def [check_for_updates](#)
- def [construct_sia_uri](#)
- def [create](#)
- def [delete](#)
- def [fetch_active](#)
- def [fetch_deprecated](#)
- def [fetch_nonnull_nonrevoked](#)

- def [fetch_pending](#)
- def [fetch_revoked](#)
- def [next_crl_number](#)
- def [next_manifest_number](#)
- def [next_serial_number](#)
- def [parent](#)
- def [rekey](#)
- def [revoke](#)

Public Attributes

- [gctx](#)
- [parent_id](#)
- [parent_resource_class](#)
- [sia_uri](#)

Static Public Attributes

- int [last_crl_sn](#) = 0
- int [last_issued_sn](#) = 0
- int [last_manifest_sn](#) = 0
- tuple [sql_template](#)

10.160.1 Detailed Description

Internal CA object.

Definition at line 299 of file rpki_engine.py.

10.160.2 Member Function Documentation

10.160.2.1 def rpki.rpki_engine.ca_obj.ca_details (*self*)

Fetch all ca_detail objects that link to this CA object.

Definition at line 321 of file rpki_engine.py.

10.160.2.2 `def rpki.rpki_engine.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 358 of file `rpki_engine.py`.

10.160.2.3 `def rpki.rpki_engine.ca_obj.construct_sia_uri (self, parent, rc)`

Construct the `sia_uri` value for this CA given configured information and the parent's up-down protocol list_response PDU.

Definition at line 345 of file `rpki_engine.py`.

10.160.2.4 `def rpki.rpki_engine.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 428 of file `rpki_engine.py`.

10.160.2.5 `def rpki.rpki_engine.ca_obj.delete (self, parent, callback)`

The list of current resource classes received from parent does not include the class corresponding to this CA, so we need to delete it (and its little dog too...).

All certs published by this CA are now invalid, so need to withdraw them, the CRL, and the manifest from the repository, delete all `child_cert` and `ca_detail` records associated with this CA, then finally delete this CA itself.

Definition at line 452 of file `rpki_engine.py`.

10.160.2.6 def rpki.rpki_engine.ca_obj.fetch_active (self)

Fetch the active ca_detail for this CA, if any.

Definition at line 329 of file rpki_engine.py.

10.160.2.7 def rpki.rpki_engine.ca_obj.fetch_deprecated (self)

Fetch deprecated ca_details for this CA, if any.

Definition at line 333 of file rpki_engine.py.

10.160.2.8 def rpki.rpki_engine.ca_obj.fetch_nonnull_nonrevoked (self)

Fetch ca_details which have a CA cert and which are not revoked.

Definition at line 341 of file rpki_engine.py.

10.160.2.9 def rpki.rpki_engine.ca_obj.fetch_pending (self)

Fetch the pending ca_details for this CA, if any.

Definition at line 325 of file rpki_engine.py.

10.160.2.10 def rpki.rpki_engine.ca_obj.fetch_revoked (self)

Fetch revoked ca_details for this CA, if any.

Definition at line 337 of file rpki_engine.py.

10.160.2.11 def rpki.rpki_engine.ca_obj.next_crl_number (self)

Allocate a CRL serial number.

Definition at line 496 of file rpki_engine.py.

10.160.2.12 def rpki.rpki_engine.ca_obj.next_manifest_number (self)

Allocate a manifest serial number.

Definition at line 488 of file rpki_engine.py.

10.160.2.13 def rpki.rpki_engine.ca_obj.next_serial_number (self)

Allocate a certificate serial number.

Definition at line 480 of file rpki_engine.py.

10.160.2.14 def rpki.rpki_engine.ca_obj.parent (self)

Fetch parent object to which this CA object links.

Definition at line 317 of file rpki_engine.py.

10.160.2.15 def rpki.rpki_engine.ca_obj.rekey (self, cb, eb)

Initiate a rekey operation for this ca. Generate a new keypair. Request cert from parent using new keypair. Mark result as our active ca_detail. Reissue all child certs issued by this ca using the new ca_detail.

Definition at line 504 of file rpki_engine.py.

10.160.2.16 def rpki.rpki_engine.ca_obj.revoke (self, cb, eb)

Revoke deprecated ca_detail objects associated with this ca.

Definition at line 529 of file rpki_engine.py.

10.160.3 Member Data Documentation**10.160.3.1 rpki.rpki_engine.ca_obj.gctx**

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 435 of file rpki_engine.py.

10.160.3.2 int rpki.rpki_engine.ca_obj.last_crl_sn = 0 [static]

Definition at line 313 of file rpki_engine.py.

10.160.3.3 int rpki.rpki_engine.ca_obj.last_issued_sn = 0 [static]

Definition at line 314 of file rpki_engine.py.

10.160.3.4 int rpki.rpki_engine.ca_obj.last_manifest_sn = 0 [static]

Definition at line 315 of file rpki_engine.py.

10.160.3.5 rpki.rpki_engine.ca_obj.parent_id

Definition at line 436 of file rpki_engine.py.

10.160.3.6 rpki.rpki_engine.ca_obj.parent_resource_class

Definition at line 437 of file rpki_engine.py.

10.160.3.7 rpki.rpki_engine.ca_obj.sia_uri

Definition at line 369 of file rpki_engine.py.

10.160.3.8 tuple rpki.rpki_engine.ca_obj.sql_template [static]

Initial value:

```
rpki.sql.template(  
    "ca",  
    "ca_id",  
    "last_crl_sn",  
    ("next_crl_update", rpki.sundial.datetime),  
    "last_issued_sn", "last_manifest_sn",  
    ("next_manifest_update", rpki.sundial.datetime),  
    "sia_uri", "parent_id", "parent_resource_class")
```

Definition at line 304 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- [rpki_engine.py \(2793\)](#)

10.161 rpki.rpki_engine.child_cert_obj Class Reference

Inherits [rpki::sql::sql_persistent](#).

Public Member Functions

- def [__init__](#)
- def [ca_detail](#)
- def [child](#)
- def [fetch](#)
- def [reissue](#)
- def [revoke](#)
- def [uri](#)
- def [uri_tail](#)

Public Attributes

- [ca_detail_id](#)
- [cert](#)
- [child_id](#)
- [gctx](#)

Static Public Attributes

- tuple [sql_template](#)

10.161.1 Detailed Description

Certificate that has been issued to a child.

Definition at line 910 of file rpki_engine.py.

10.161.2 Member Function Documentation

10.161.2.1 `def rpki.rpki_engine.child_cert_obj.__init__ (self, gctx = None, child_id = None, ca_detail_id = None, cert = None)`

Initialize a child_cert_obj.

Definition at line 923 of file rpki_engine.py.

10.161.2.2 `def rpki.rpki_engine.child_cert_obj.ca_detail (self)`

Fetch ca_detail object to which this child_cert object links.

Definition at line 939 of file rpki_engine.py.

10.161.2.3 `def rpki.rpki_engine.child_cert_obj.child (self)`

Fetch child object to which this child_cert object links.

Definition at line 935 of file rpki_engine.py.

10.161.2.4 `def rpki.rpki_engine.child_cert_obj.fetch (cls, gctx = None, child = None, ca_detail = None, ski = None, unique = False)`

Fetch all child_cert objects matching a particular set of parameters. This is a wrapper to consolidate various queries that would otherwise be inline SQL WHERE expressions. In most cases code calls this indirectly, through methods in other classes.

Definition at line 1041 of file rpki_engine.py.

10.161.2.5 `def rpki.rpki_engine.child_cert_obj.reissue (self, ca_detail, callback, errback, resources = None, sia = None)`

Reissue an existing cert, reusing the public key. If the 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 certificate 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 972 of file rpki_engine.py.

10.161.2.6 `def rpki.rpki_engine.child_cert_obj.revoke (self, callback, errback, withdraw = True)`

Revoke a child cert.

Definition at line 951 of file rpki_engine.py.

10.161.2.7 `def rpki.rpki_engine.child_cert_obj.uri (self, ca)`

Return the publication URI for this child_cert.

Definition at line 947 of file rpki_engine.py.

10.161.2.8 def rpki.rpki_engine.child_cert_obj.uri_tail (*self*)

Return the tail (filename) portion of the URI for this child_cert.

Definition at line 943 of file rpki_engine.py.

10.161.3 Member Data Documentation**10.161.3.1 rpki.rpki_engine.child_cert_obj.ca_detail_id**

Definition at line 930 of file rpki_engine.py.

10.161.3.2 rpki.rpki_engine.child_cert_obj.cert

Definition at line 931 of file rpki_engine.py.

10.161.3.3 rpki.rpki_engine.child_cert_obj.child_id

Definition at line 929 of file rpki_engine.py.

10.161.3.4 rpki.rpki_engine.child_cert_obj.gctx

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 928 of file rpki_engine.py.

10.161.3.5 tuple rpki.rpki_engine.child_cert_obj.sql_template [static]**Initial value:**

```
rpki.sql.template(  
    "child_cert",  
    "child_cert_id",
```

```
("cert", rpki.x509.X509),  
"child_id",  
"ca_detail_id",  
"ski")
```

Definition at line 915 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- [rpki_engine.py \(2793\)](#)

10.162 rpki.rpki_engine.revoked_cert_obj Class Reference

Inherits [rpki::sql::sql_persistent](#).

Public Member Functions

- [def __init__](#)
- [def ca_detail](#)
- [def revoke](#)

Public Attributes

- [ca_detail_id](#)
- [expires](#)
- [gctx](#)
- [revoked](#)
- [serial](#)

Static Public Attributes

- tuple [sql_template](#)

10.162.1 Detailed Description

Tombstone for a revoked certificate.

Definition at line 1073 of file rpki_engine.py.

10.162.2 Member Function Documentation

10.162.2.1 `def rpki.rpki_engine.revoked_cert_obj.__init__ (self, gctx = None, serial = None, revoked = None, expires = None, ca_detail_id = None)`

Initialize a `revoked_cert_obj`.

Definition at line 1086 of file `rpki_engine.py`.

10.162.2.2 `def rpki.rpki_engine.revoked_cert_obj.ca_detail (self)`

Fetch `ca_detail` object to which this `revoked_cert_obj` links.

Definition at line 1097 of file `rpki_engine.py`.

10.162.2.3 `def rpki.rpki_engine.revoked_cert_obj.revoke (cls, cert, ca_detail)`

Revoke a certificate.

Definition at line 1102 of file `rpki_engine.py`.

10.162.3 Member Data Documentation

10.162.3.1 `rpki.rpki_engine.revoked_cert_obj.ca_detail_id`

Definition at line 1093 of file `rpki_engine.py`.

10.162.3.2 `rpki.rpki_engine.revoked_cert_obj.expires`

Definition at line 1092 of file `rpki_engine.py`.

10.162.3.3 rpki.rpki_engine.revoked_cert_obj.gctx

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 1089 of file rpki_engine.py.

10.162.3.4 rpki.rpki_engine.revoked_cert_obj.revoked

Definition at line 1091 of file rpki_engine.py.

10.162.3.5 rpki.rpki_engine.revoked_cert_obj.serial

Definition at line 1090 of file rpki_engine.py.

10.162.3.6 tuple rpki.rpki_engine.revoked_cert_obj.sql_template [static]

Initial value:

```
rpki.sql.template(  
    "revoked_cert",  
    "revoked_cert_id",  
    "serial",  
    "ca_detail_id",  
    ("revoked", rpki.sundial.datetime),  
    ("expires", rpki.sundial.datetime))
```

Definition at line 1078 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- [rpki_engine.py \(2793\)](#)

10.163 rpki.rpki_engine.roa_obj Class Reference

Inherits [rpki::sql::sql_persistent](#).

Public Member Functions

- [def __init__](#)

- def [ca_detail](#)
- def [generate](#)
- def [regenerate](#)
- def [revoke](#)
- def [self](#)
- def [sql_delete_hook](#)
- def [sql_fetch_hook](#)
- def [sql_insert_hook](#)
- def [update](#)
- def [uri](#)
- def [uri_tail](#)

Public Attributes

- [asn](#)
- [gctx](#)
- [ipv4](#)
- [ipv6](#)
- [self_id](#)

Static Public Attributes

- [ca_detail_id](#) = None
- [cert](#) = None
- [roa](#) = None
- tuple [sql_template](#)

10.163.1 Detailed Description

Route Origin Authorization.

Definition at line 1113 of file `rpki_engine.py`.

10.163.2 Member Function Documentation

10.163.2.1 `def rpki.rpki_engine.roa_obj.__init__ (self, gctx = None, self_id = None, asn = None, ipv4 = None, ipv6 = None)`

Definition at line 1177 of file `rpki_engine.py`.

10.163.2.2 def rpki.rpki_engine.roa_obj.ca_detail (self)

Fetch ca_detail object to which this roa_obj links.

Definition at line 1137 of file rpki_engine.py.

10.163.2.3 def rpki.rpki_engine.roa_obj.generate (self, callback, errback)

Generate a ROA.

At present this does not support ROAs with multiple signatures (neither does the current CMS code).

At present we have no way of performing a direct lookup from a desired set of resources to a covering certificate, so we have to search. This could be quite slow if we have a lot of active ca_detail objects. Punt on the issue for now, revisit if profiling shows this as a hotspot.

Once we have the right covering certificate, we generate the ROA payload, generate a new EE certificate, use the EE certificate to sign the ROA payload, publish the result, then throw away the private key for the EE cert, all per the ROA specification. This implies that generating a lot of ROAs will tend to thrash /dev/random, but there is not much we can do about that.

Definition at line 1228 of file rpki_engine.py.

10.163.2.4 def rpki.rpki_engine.roa_obj.regenerate (self, callback, errback)

Reissue ROA associated with this roa_obj.

Definition at line 1335 of file rpki_engine.py.

10.163.2.5 def rpki.rpki_engine.roa_obj.revoke (self, callback, errback, regenerate = False, allow_failure = False)

Withdraw ROA associated with this roa_obj.

In order to preserve make-before-break properties without duplicating code, this method also handles generating a replacement ROA when requested.

Definition at line 1297 of file rpki_engine.py.

10.163.2.6 def rpki.rpki_engine.roa_obj.self (self)

Fetch self object to which this roa_obj links.

Definition at line 1131 of file rpki_engine.py.

10.163.2.7 def rpki.rpki_engine.roa_obj.sql_delete_hook (self)

Extra SQL delete actions for roa_obj -- handle prefix lists.

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 1171 of file rpki_engine.py.

10.163.2.8 def rpki.rpki_engine.roa_obj.sql_fetch_hook (self)

Extra SQL fetch actions for roa_obj -- handle prefix lists.

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 1143 of file rpki_engine.py.

10.163.2.9 def rpki.rpki_engine.roa_obj.sql_insert_hook (self)

Extra SQL insert actions for roa_obj -- handle prefix lists.

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 1157 of file rpki_engine.py.

10.163.2.10 `def rpki.rpki_engine.roa_obj.update (self, callback, errback)`

Bring this roa_obj's ROA up to date if necessary.

Definition at line 1196 of file rpki_engine.py.

10.163.2.11 `def rpki.rpki_engine.roa_obj.uri (self, key = None)`

Return the publication URI for this roa_obj's ROA.

Definition at line 1344 of file rpki_engine.py.

10.163.2.12 `def rpki.rpki_engine.roa_obj.uri_tail (self, key = None)`

Return the tail (filename portion) of the publication URI for this roa_obj's ROA.

Definition at line 1350 of file rpki_engine.py.

10.163.3 Member Data Documentation**10.163.3.1** `rpki.rpki_engine.roa_obj.asn`

Definition at line 1181 of file rpki_engine.py.

10.163.3.2 `rpki.rpki_engine.roa_obj.ca_detail_id = None` `[static]`

Definition at line 1127 of file rpki_engine.py.

10.163.3.3 `rpki.rpki_engine.roa_obj.cert = None` `[static]`

Definition at line 1128 of file rpki_engine.py.

10.163.3.4 rpki.rpki_engine.roa_obj.gctx

Reimplemented from [rpki.sql.sql_persistent](#).
Definition at line 1179 of file rpki_engine.py.

10.163.3.5 rpki.rpki_engine.roa_obj.ipv4

Definition at line 1182 of file rpki_engine.py.

10.163.3.6 rpki.rpki_engine.roa_obj.ipv6

Definition at line 1183 of file rpki_engine.py.

10.163.3.7 rpki.rpki_engine.roa_obj.roa = None [static]

Definition at line 1129 of file rpki_engine.py.

10.163.3.8 rpki.rpki_engine.roa_obj.self_id

Definition at line 1180 of file rpki_engine.py.

10.163.3.9 tuple rpki.rpki_engine.roa_obj.sql_template [static]

Initial value:

```
rpki.sql.template(  
    "roa",  
    "roa_id",  
    "ca_detail_id",  
    "self_id",  
    "asn",  
    ("roa", rpki.x509.ROA),  
    ("cert", rpki.x509.X509))
```

Definition at line 1118 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- [rpki_engine.py \(2793\)](#)

10.164 rpki.rpki_engine.rpkid_context Class Reference

Inherits [object](#).

Public Member Functions

- [def __init__](#)
- [def build_https_ta_cache](#)
- [def clear_https_ta_cache](#)
- [def cron](#)
- [def cronjob_handler](#)
- [def irdb_query](#)
- [def irdb_query_child_resources](#)
- [def irdb_query_roa_requests](#)
- [def left_right_handler](#)
- [def start_cron](#)
- [def up_down_handler](#)

Public Attributes

- [bpki_ta](#)
- [cron_keepalive](#)
- [cron_period](#)
- [cron_timeout](#)
- [https_server_host](#)
- [https_server_port](#)
- [initial_delay](#)
- [irbe_cert](#)
- [irdb_cert](#)
- [irdb_url](#)
- [publication_kludge_base](#)
- [rpkid_cert](#)
- [rpkid_key](#)
- [sql](#)
- [use_internal_cron](#)

Static Public Attributes

- `https_ta_cache` = None
HTTPS trust anchor cache, to avoid regenerating it for every TLS connection.
- tuple `up_down_url_regexp` = `re.compile("/up-down/([-A-Z0-9_]+)/([-A-Z0-9_-]+)$", re.I)`

10.164.1 Detailed Description

A container for various global rpkid parameters.

Definition at line 39 of file `rpki_engine.py`.

10.164.2 Member Function Documentation

10.164.2.1 `def rpki.rpki_engine.rpkid_context.__init__ (self, cfg)`

Definition at line 44 of file `rpki_engine.py`.

10.164.2.2 `def rpki.rpki_engine.rpkid_context.build_https_ta_cache (self)`

Build dynamic TLS trust anchors.

Definition at line 279 of file `rpki_engine.py`.

10.164.2.3 `def rpki.rpki_engine.rpkid_context.clear_https_ta_cache (self)`

Clear dynamic TLS trust anchors.

Definition at line 270 of file `rpki_engine.py`.

10.164.2.4 `def rpki.rpki_engine.rpkid_context.cron (self, cb = None)`

Periodic tasks.

Definition at line 199 of file rpki_engine.py.

10.164.2.5 `def rpki.rpki_engine.rpkid_context.cronjob_handler (self, query,
path, cb)`

External trigger for periodic tasks. This is somewhat obsolete now that we have internal timers, but the test framework still uses it.

Definition at line 254 of file rpki_engine.py.

10.164.2.6 `def rpki.rpki_engine.rpkid_context.irdb_query (self, q_pdu,
callback, errback)`

Perform an IRDB callback query.

Definition at line 85 of file rpki_engine.py.

10.164.2.7 `def rpki.rpki_engine.rpkid_context.irdb_query_child_resources (self, self_handle, child_handle, callback, errback)`

Ask IRDB about a child's resources.

Definition at line 111 of file rpki_engine.py.

10.164.2.8 `def rpki.rpki_engine.rpkid_context.irdb_query_roa_requests (self,
self_handle, callback, errback)`

Ask IRDB about self's ROA requests.

Definition at line 133 of file rpki_engine.py.

10.164.2.9 `def rpki.rpki_engine.rpkid_context.left_right_handler (self, query, path, cb)`

Process one left-right PDU.

Definition at line 145 of file rpki_engine.py.

10.164.2.10 `def rpki.rpki_engine.rpkid_context.start_cron (self)`

Start clock for rpkid's internal cron process.

Definition at line 73 of file rpki_engine.py.

10.164.2.11 `def rpki.rpki_engine.rpkid_context.up_down_handler (self, query, path, cb)`

Process one up-down PDU.

Definition at line 171 of file rpki_engine.py.

10.164.3 Member Data Documentation**10.164.3.1** `rpki.rpki_engine.rpkid_context.bpki_ta`

Definition at line 48 of file rpki_engine.py.

10.164.3.2 `rpki.rpki_engine.rpkid_context.cron_keepalive`

Definition at line 68 of file rpki_engine.py.

10.164.3.3 `rpki.rpki_engine.rpkid_context.cron_period`

Definition at line 67 of file rpki_engine.py.

10.164.3.4 rpki.rpki_engine.rpkid_context.cron_timeout

Definition at line 71 of file rpki_engine.py.

10.164.3.5 rpki.rpki_engine.rpkid_context.https_server_host

Definition at line 56 of file rpki_engine.py.

10.164.3.6 rpki.rpki_engine.rpkid_context.https_server_port

Definition at line 57 of file rpki_engine.py.

10.164.3.7 rpki::rpki_engine.rpkid_context::https_ta_cache = None
[static]

HTTPS trust anchor cache, to avoid regenerating it for every TLS connection.

Definition at line 268 of file rpki_engine.py.

10.164.3.8 rpki.rpki_engine.rpkid_context.initial_delay

Definition at line 63 of file rpki_engine.py.

10.164.3.9 rpki.rpki_engine.rpkid_context.irbe_cert

Definition at line 50 of file rpki_engine.py.

10.164.3.10 rpki.rpki_engine.rpkid_context.irdb_cert

Definition at line 49 of file rpki_engine.py.

10.164.3.11 rpki.rpki_engine.rpkid_context.irdb_url

Definition at line 54 of file rpki_engine.py.

10.164.3.12 rpki.rpki_engine.rpkid_context.publication_kludge_base

Definition at line 59 of file rpki_engine.py.

10.164.3.13 rpki.rpki_engine.rpkid_context.rpkid_cert

Definition at line 51 of file rpki_engine.py.

10.164.3.14 rpki.rpki_engine.rpkid_context.rpkid_key

Definition at line 52 of file rpki_engine.py.

10.164.3.15 rpki.rpki_engine.rpkid_context.sql

Definition at line 46 of file rpki_engine.py.

**10.164.3.16 tuple rpki.rpki_engine.rpkid_context.up_down_url_regexp =
re.compile("/up-down/([-A-Z0-9_]+)/([-A-Z0-9_]+)\$", re.I)
[static]**

Definition at line 169 of file rpki_engine.py.

10.164.3.17 rpki.rpki_engine.rpkid_context.use_internal_cron

Definition at line 61 of file rpki_engine.py.

The documentation for this class was generated from the following file:

- [rpki_engine.py \(2793\)](#)

10.165 rpki.sql.session Class Reference

Inherits [object](#).

Public Member Functions

- [def __init__](#)
- [def assert_pristine](#)
- [def cache_clear](#)
- [def close](#)
- [def connect](#)
- [def execute](#)
- [def executemany](#)
- [def fetchall](#)
- [def lastrowid](#)
- [def ping](#)
- [def sweep](#)

Public Attributes

- [cache](#)
- [cur](#)
- [database](#)
- [db](#)
- [dirty](#)
- [password](#)
- [username](#)

Private Member Functions

- [def _wrap_execute](#)

Static Private Attributes

- [_exceptions_enabled](#) = False

10.165.1 Detailed Description

SQL session layer.

Definition at line 38 of file sql.py.

10.165.2 Member Function Documentation

10.165.2.1 def rpki.sql.session.__init__ (*self*, *cfg*)

Definition at line 45 of file sql.py.

10.165.2.2 def rpki.sql.session._wrap_execute (*self*, *func*, *query*, *args*) [private]

Definition at line 76 of file sql.py.

10.165.2.3 def rpki.sql.session.assert_pristine (*self*)

Assert that there are no dirty objects in the cache.

Definition at line 100 of file sql.py.

10.165.2.4 def rpki.sql.session.cache_clear (*self*)

Clear the object cache.

Definition at line 96 of file sql.py.

10.165.2.5 def rpki.sql.session.close (*self*)

Definition at line 65 of file sql.py.

10.165.2.6 def rpki.sql.session.connect (*self*)

Definition at line 60 of file sql.py.

10.165.2.7 def rpki.sql.session.execute (*self*, *query*, *args* = None)

Definition at line 84 of file sql.py.

10.165.2.8 def rpki.sql.session.executemany (*self*, *query*, *args*)

Definition at line 87 of file sql.py.

10.165.2.9 def rpki.sql.session.fetchall (*self*)

Definition at line 90 of file sql.py.

10.165.2.10 def rpki.sql.session.lastrowid (*self*)

Definition at line 93 of file sql.py.

10.165.2.11 def rpki.sql.session.ping (*self*)

Definition at line 73 of file sql.py.

10.165.2.12 def rpki.sql.session.sweep (*self*)

Write any dirty objects out to SQL.

Definition at line 104 of file sql.py.

10.165.3 Member Data Documentation

10.165.3.1 `rpki.sql.session._exceptions_enabled = False` [static, private]

Definition at line 43 of file sql.py.

10.165.3.2 `rpki.sql.session.cache`

Definition at line 55 of file sql.py.

10.165.3.3 `rpki.sql.session.cur`

Definition at line 62 of file sql.py.

10.165.3.4 `rpki.sql.session.database`

Definition at line 52 of file sql.py.

10.165.3.5 `rpki.sql.session.db`

Definition at line 61 of file sql.py.

10.165.3.6 `rpki.sql.session.dirty`

Definition at line 56 of file sql.py.

10.165.3.7 `rpki.sql.session.password`

Definition at line 53 of file sql.py.

10.165.3.8 rpki.sql.session.username

Definition at line 51 of file sql.py.

The documentation for this class was generated from the following file:

- [sql.py \(2648\)](#)

10.166 rpki.sql.sql_persistent Class Reference

Inherits [object](#).

Inherited by [rpki.left_right.data_elt](#), [rpki.publication.control_elt](#), [rpki.rpki_engine.ca_detail_obj](#), [rpki.rpki_engine.ca_obj](#), [rpki.rpki_engine.child_cert_obj](#), [rpki.rpki_engine.revoked_cert_obj](#), and [rpki.rpki_engine.roa_obj](#).

Public Member Functions

- def [sql_decode](#)
- def [sql_delete](#)
- def [sql_delete_hook](#)
- def [sql_encode](#)
- def [sql_fetch](#)
- def [sql_fetch_all](#)
- def [sql_fetch_hook](#)
- def [sql_fetch_where](#)
- def [sql_fetch_where1](#)
- def [sql_init](#)
- def [sql_insert_hook](#)
- def [sql_is_dirty](#)
- def [sql_mark_clean](#)
- def [sql_mark_deleted](#)
- def [sql_mark_dirty](#)
- def [sql_store](#)
- def [sql_update_hook](#)

Public Attributes

- [gctx](#)

Static Public Attributes

- `sql_debug` = False
Enable logging of SQL actions.
- `sql_deleted` = False
*Whether our cached copy of this *object* has been deleted.*
- `sql_in_db` = False
*Whether this *object* is already in SQL or not.*

10.166.1 Detailed Description

Mixin for persistent class that needs to be stored in SQL.

Definition at line 140 of file sql.py.

10.166.2 Member Function Documentation

10.166.2.1 `def rpki.sql.sql_persistent.sql_decode (self, vals)`

Initialize an object with values returned by `self.sql_fetch()`.
This is a default version that assumes a one-to-one mapping between column names in SQL and attribute names in Python. If you need something fancier, override this.

Reimplemented in `rpki.rpki_engine.ca_detail_obj`.

Definition at line 310 of file sql.py.

10.166.2.2 `def rpki.sql.sql_persistent.sql_delete (self)`

Delete this object from SQL.

Definition at line 281 of file sql.py.

10.166.2.3 def rpki.sql.sql_persistent.sql_delete_hook (self)

Customization hook.

Reimplemented in [rpki.rpki_engine.roa_obj](#).

Definition at line 336 of file sql.py.

10.166.2.4 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 297 of file sql.py.

10.166.2.5 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 161 of file sql.py.

10.166.2.6 def rpki.sql.sql_persistent.sql_fetch_all (cls, gctx)

Fetch all objects of this type from SQL.

Definition at line 199 of file sql.py.

10.166.2.7 `def rpki.sql.sql_persistent.sql_fetch_hook (self)`

Customization hook.

Reimplemented in [rpki.rpki_engine.roa_obj](#).

Definition at line 323 of file sql.py.

10.166.2.8 `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 204 of file sql.py.

10.166.2.9 `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 184 of file sql.py.

10.166.2.10 `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 231 of file sql.py.

10.166.2.11 `def rpki.sql.sql_persistent.sql_insert_hook (self)`

Customization hook.

Reimplemented in [rpki.rpki_engine.roa_obj](#).

Definition at line 327 of file sql.py.

10.166.2.12 def rpki.sql.sql_persistent.sql_is_dirty (*self*)

Query whether this object needs to be written back to SQL.

Definition at line 251 of file sql.py.

10.166.2.13 def rpki.sql.sql_persistent.sql_mark_clean (*self*)

Mark this object as not needing to be written back to SQL.

Definition at line 247 of file sql.py.

10.166.2.14 def rpki.sql.sql_persistent.sql_mark_deleted (*self*)

Mark this object as needing to be deleted in SQL.

Definition at line 255 of file sql.py.

10.166.2.15 def rpki.sql.sql_persistent.sql_mark_dirty (*self*)

Mark this object as needing to be written back to SQL.

Definition at line 243 of file sql.py.

10.166.2.16 def rpki.sql.sql_persistent.sql_store (*self*)

Store this object to SQL.

Definition at line 259 of file sql.py.

10.166.2.17 `def rpki.sql.sql_persistent.sql_update_hook (self)`

Customization hook.

Definition at line 331 of file sql.py.

10.166.3 Member Data Documentation**10.166.3.1** `rpki.sql.sql_persistent.gctx`

Reimplemented in [rpki.rpki_engine.ca_obj](#), [rpki.rpki_engine.ca_detail_obj](#), [rpki.rpki_engine.child_cert_obj](#), [rpki.rpki_engine.revoked_cert_obj](#), and [rpki.rpki_engine.roa_obj](#).

Definition at line 236 of file sql.py.

10.166.3.2 `rpki::sql.sql_persistent::sql_debug = False` `[static]`

Enable logging of SQL actions.

Definition at line 158 of file sql.py.

10.166.3.3 `rpki::sql.sql_persistent::sql_deleted = False` `[static]`

Whether our cached copy of this [object](#) has been deleted.

Definition at line 153 of file sql.py.

10.166.3.4 `rpki::sql.sql_persistent::sql_in_db = False` `[static]`

Whether this [object](#) is already in SQL or not.

Definition at line 148 of file sql.py.

The documentation for this class was generated from the following file:

- [sql.py \(2648\)](#)

10.167 rpki.sql.template Class Reference

Inherits [object](#).

Public Member Functions

- [def __init__](#)

Public Attributes

- [columns](#)
- [delete](#)
- [index](#)
- [insert](#)
- [map](#)
- [select](#)
- [table](#)
- [update](#)

10.167.1 Detailed Description

SQL template generator.

Definition at line 116 of file sql.py.

10.167.2 Member Function Documentation

10.167.2.1 `def rpki.sql.template.__init__ (self, table_name, index_column, data_columns)`

Build a SQL template.

Definition at line 121 of file sql.py.

10.167.3 Member Data Documentation

10.167.3.1 `rpki.sql.template.columns`

Definition at line 128 of file sql.py.

10.167.3.2 rpki.sql.template.delete

Definition at line 138 of file sql.py.

10.167.3.3 rpki.sql.template.index

Definition at line 127 of file sql.py.

10.167.3.4 rpki.sql.template.insert

Definition at line 131 of file sql.py.

10.167.3.5 rpki.sql.template.map

Definition at line 129 of file sql.py.

10.167.3.6 rpki.sql.template.select

Definition at line 130 of file sql.py.

10.167.3.7 rpki.sql.template.table

Definition at line 126 of file sql.py.

10.167.3.8 rpki.sql.template.update

Definition at line 134 of file sql.py.

The documentation for this class was generated from the following file:

- [sql.py \(2648\)](#)

10.168 rpki.sundial.datetime Class Reference

Inherits [pydatetime::datetime](#).

Public Member Functions

- def [__add__](#)
- def [__radd__](#)
- def [__rsub__](#)
- def [__str__](#)
- def [__sub__](#)
- def [earlier](#)
- def [from_sql](#)
- def [fromASN1tuple](#)
- def [fromdatetime](#)
- def [fromGeneralizedTime](#)
- def [fromUTCTime](#)
- def [fromXMLtime](#)
- def [later](#)
- def [to_sql](#)
- def [toASN1tuple](#)
- def [toGeneralizedTime](#)
- def [timestamp](#)
- def [toUTCTime](#)
- def [toXMLtime](#)

Static Public Attributes

- tuple [PKIX_threshold](#) = [pydatetime.datetime](#)(2050, 1, 1)
Threshold specified in RFC 3280 for switchover from UTCTime to GeneralizedTime.

10.168.1 Detailed Description

RPKI extensions to standard `datetime.datetime` class. All work here is in UTC, so we use naive datetime objects.

Definition at line 54 of file `sundial.py`.

10.168.2 Member Function Documentation

10.168.2.1 def rpki.sundial.datetime.__add__ (x, y)

Definition at line 163 of file sundial.py.

10.168.2.2 def rpki.sundial.datetime.__radd__ (x, y)

Definition at line 164 of file sundial.py.

10.168.2.3 def rpki.sundial.datetime.__rsub__ (x, y)

Definition at line 165 of file sundial.py.

10.168.2.4 def rpki.sundial.datetime.__str__ (self)

Definition at line 124 of file sundial.py.

10.168.2.5 def rpki.sundial.datetime.__sub__ (x, y)

Definition at line 166 of file sundial.py.

10.168.2.6 def rpki.sundial.datetime.earlier (self, other)

Return the earlier of two timestamps.

Definition at line 159 of file sundial.py.

10.168.2.7 def rpki.sundial.datetime.from_sql (cls, x)

Convert from SQL storage format.

Definition at line 136 of file sundial.py.

10.168.2.8 def rpki.sundial.datetime.fromASN1tuple (cls, x)

Convert from ASN.1 tuple representation.

Definition at line 86 of file sundial.py.

10.168.2.9 def rpki.sundial.datetime.fromdatetime (cls, x)

Convert a datetime.datetime object into this subclass. This is whacky due to the weird constructors for datetime.

Definition at line 128 of file sundial.py.

10.168.2.10 def rpki.sundial.datetime.fromGeneralizedTime (cls, x)

Convert from ASN.1 GeneralizedTime.

Definition at line 77 of file sundial.py.

10.168.2.11 def rpki.sundial.datetime.fromUTCTime (cls, x)

Convert from ASN.1 UTCTime.

Definition at line 68 of file sundial.py.

10.168.2.12 def rpki.sundial.datetime.fromXMLtime (cls, x)

Convert from XML time representation.

Definition at line 111 of file sundial.py.

10.168.2.13 def rpki.sundial.datetime.later (self, other)

Return the later of two timestamps.

Definition at line 155 of file sundial.py.

10.168.2.14 def rpki.sundial.datetime.to_sql (self)

Convert to SQL storage format.

There's something whacky going on in the MySQLdb module, it throws range errors when storing a derived type into a DATETIME column. Investigate some day, but for now brute force this by copying the relevant fields into a datetime.datetime for MySQLdb's consumption.

Definition at line 140 of file sundial.py.

10.168.2.15 def rpki.sundial.datetime.toASN1tuple (self)

Convert to ASN.1 tuple representation.

Definition at line 101 of file sundial.py.

10.168.2.16 def rpki.sundial.datetime.toGeneralizedTime (self)

Convert to ASN.1 GeneralizedTime.

Definition at line 81 of file sundial.py.

10.168.2.17 def rpki.sundial.datetime.totimestamp (self)

Convert to seconds from epoch (like time.time()). Conversion method is a bit silly, but avoids time module timezone whackiness.

Definition at line 60 of file sundial.py.

10.168.2.18 def rpki.sundial.datetime.toUTCTime (self)

Convert to ASN.1 UTCTime.

Definition at line 72 of file sundial.py.

10.168.2.19 def rpki.sundial.datetime.toXMLtime (self)

Convert to XML time representation.

Definition at line 120 of file sundial.py.

10.168.3 Member Data Documentation**10.168.3.1 rpki::sundial.datetime::PKIX_threshold =
pydatetime.datetime(2050, 1, 1) [static]**

Threshold specified in RFC 3280 for switchover from UTCTime to GeneralizedTime.

Definition at line 99 of file sundial.py.

The documentation for this class was generated from the following file:

- [sundial.py \(2785\)](#)

10.169 rpki.sundial.timedelta Class Reference

Inherits [pydatetime::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.

10.169.1 Detailed Description

Timedelta with text parsing. This accepts two input formats:

- A simple integer, indicating a number of seconds.
- A string of the form "wD xH yM zS" where w, x, y, and z are integers and D, H, M, and S indicate 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".

Definition at line 168 of file sundial.py.

10.169.2 Member Function Documentation

10.169.2.1 def rpki.sundial.timedelta.__abs__ (x)

Definition at line 218 of file sundial.py.

10.169.2.2 def rpki.sundial.timedelta.__add__ (x, y)

Definition at line 219 of file sundial.py.

10.169.2.3 def rpki.sundial.timedelta.__div__ (x, y)

Definition at line 220 of file sundial.py.

10.169.2.4 def rpki.sundial.timedelta.__floordiv__ (x, y)

Definition at line 221 of file sundial.py.

10.169.2.5 def rpki.sundial.timedelta.__mul__ (x, y)

Definition at line 222 of file sundial.py.

10.169.2.6 def rpki.sundial.timedelta.__neg__ (x)

Definition at line 223 of file sundial.py.

10.169.2.7 def rpki.sundial.timedelta.__pos__ (x)

Definition at line 224 of file sundial.py.

10.169.2.8 def rpki.sundial.timedelta.__radd__ (x, y)

Definition at line 225 of file sundial.py.

10.169.2.9 def rpki.sundial.timedelta.__rdiv__ (x, y)

Definition at line 226 of file sundial.py.

10.169.2.10 def rpki.sundial.timedelta.__rfloordiv__ (x, y)

Definition at line 227 of file sundial.py.

10.169.2.11 def rpki.sundial.timedelta.__rmul__ (x, y)

Definition at line 228 of file sundial.py.

10.169.2.12 def rpki.sundial.timedelta.__rsub__ (x, y)

Definition at line 229 of file sundial.py.

10.169.2.13 def rpki.sundial.timedelta.__sub__ (x, y)

Definition at line 230 of file sundial.py.

10.169.2.14 def rpki.sundial.timedelta.convert_to_seconds (self)

Convert a timedelta interval to seconds.

Definition at line 209 of file sundial.py.

10.169.2.15 def rpki.sundial.timedelta.fromtimedelta (cls, x)

Convert a datetime.timedelta object into this subclass.

Definition at line 214 of file sundial.py.

10.169.2.16 def rpki.sundial.timedelta.parse (cls, arg)

Parse text into a timedelta object.

Definition at line 194 of file sundial.py.

10.169.3 Member Data Documentation

10.169.3.1 rpki::sundial.timedelta::regex [static]

Initial value:

```
re.compile("\\s*".join(("^",
                        "(?: (?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 185 of file sundial.py.

The documentation for this class was generated from the following file:

- [sundial.py \(2785\)](#)

10.170 rpki.up_down.base_elt Class Reference

Inherits [object](#).

Inherited by [rpki.up_down.certificate_elt](#), [rpki.up_down.class_elt](#), [rpki.up_down.class_response_syntax](#), [rpki.up_down.error_response_pdu](#), [rpki.up_down.issue_pdu](#), [rpki.up_down.list_pdu](#), [rpki.up_down.message_pdu](#), and [rpki.up_down.revoke_syntax](#).

Public Member Functions

- def [check_response](#)
- def [endElement](#)
- def [make_b64elt](#)
- def [make_elt](#)
- def [serve_pdu](#)
- def [startElement](#)

10.170.1 Detailed Description

Generic PDU object.

Virtual class, just provides some default methods.

Definition at line 43 of file up_down.py.

10.170.2 Member Function Documentation

10.170.2.1 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.

10.170.2.2 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.

10.170.2.3 def rpki.up_down.base_elt.make_b64elt (self, elt, name, value = None)

Construct a sub-element with Base64 text content.

Definition at line 78 of file up_down.py.

10.170.2.4 `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`.

10.170.2.5 `def rpki.up_down.base_elt.serve_pdu (self, q_msg, r_msg, child, callback, errback)`

Default PDU handler to catch unexpected types.

Reimplemented in [rpki.up_down.list_pdu](#), [rpki.up_down.issue_pdu](#), [rpki.up_down.revoke_pdu](#), [rootd.list_pdu](#), [rootd.issue_pdu](#), and [rootd.revoke_pdu](#).

Definition at line 87 of file `up_down.py`.

10.170.2.6 `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 \(2793\)](#)

10.171 `rpki.up_down.certificate_elt` Class Reference

Inherits [rpki::up_down::base_elt](#).

Public Member Functions

- def [endElement](#)
- def [startElement](#)
- def [toXML](#)

Public Attributes

- [cert](#)
- [cert_url](#)
- [req_resource_set_as](#)
- [req_resource_set_ipv4](#)
- [req_resource_set_ipv6](#)

10.171.1 Detailed Description

Up-Down protocol representation of an issued certificate.

Definition at line 128 of file up_down.py.

10.171.2 Member Function Documentation

10.171.2.1 def rpki.up_down.certificate_elt.endElement (*self*, *stack*, *name*, *text*)

Handle text content of a <certificate/> element.

Reimplemented from [rpki.up_down.base_elt](#).

Definition at line 143 of file up_down.py.

10.171.2.2 def rpki.up_down.certificate_elt.startElement (*self*, *stack*, *name*, *attrs*)

Handle attributes of <certificate/> element.

Reimplemented from [rpki.up_down.base_elt](#).

Definition at line 133 of file up_down.py.

10.171.2.3 def rpki.up_down.certificate_elt.toXML (*self*)

Generate a <certificate/> element.

Definition at line 151 of file up_down.py.

10.171.3 Member Data Documentation

10.171.3.1 rpki.up_down.certificate_elt.cert

Definition at line 148 of file up_down.py.

10.171.3.2 rpki.up_down.certificate_elt.cert_url

Definition at line 138 of file up_down.py.

10.171.3.3 rpki.up_down.certificate_elt.req_resource_set_as

Definition at line 139 of file up_down.py.

10.171.3.4 rpki.up_down.certificate_elt.req_resource_set_ipv4

Definition at line 140 of file up_down.py.

10.171.3.5 rpki.up_down.certificate_elt.req_resource_set_ipv6

Definition at line 141 of file up_down.py.

The documentation for this class was generated from the following file:

- [up_down.py \(2793\)](#)

10.172 rpki.up_down.class_elt Class Reference

Inherits [rpki::up_down::base_elt](#).

Public Member Functions

- [def __init__](#)
- [def endElement](#)
- [def from_resource_bag](#)
- [def startElement](#)
- [def to_resource_bag](#)
- [def toXML](#)

Public Attributes

- [cert_url](#)
- [certs](#)
- [class_name](#)
- [resource_set_as](#)
- [resource_set_ipv4](#)
- [resource_set_ipv6](#)
- [resource_set_notafter](#)
- [suggested_sia_head](#)

Static Public Attributes

- [issuer](#) = None

10.172.1 Detailed Description

Up-Down protocol representation of a resource class.

Definition at line 160 of file up_down.py.

10.172.2 Member Function Documentation

10.172.2.1 def rpki.up_down.class_elt.__init__ (self)

Initialize class_elt.

Definition at line 167 of file up_down.py.

10.172.2.2 def rpki.up_down.class_elt.endElement (*self*, *stack*, *name*, *text*)

Handle <class/> elements and their children.

Reimplemented from [rpki.up_down.base_elt](#).

Definition at line 191 of file up_down.py.

10.172.2.3 def rpki.up_down.class_elt.from_resource_bag (*self*, *bag*)

Set resources of this class element from a resource_bag.

Definition at line 222 of file up_down.py.

10.172.2.4 def rpki.up_down.class_elt.startElement (*self*, *stack*, *name*, *attrs*)

Handle <class/> elements and their children.

Reimplemented from [rpki.up_down.base_elt](#).

Definition at line 172 of file up_down.py.

10.172.2.5 def rpki.up_down.class_elt.to_resource_bag (*self*)

Build a resource_bag from from this <class/> element.

Definition at line 213 of file up_down.py.

10.172.2.6 def rpki.up_down.class_elt.toXML (*self*)

Generate a <class/> element.

Definition at line 201 of file up_down.py.

10.172.3 Member Data Documentation

10.172.3.1 rpki.up_down.class_elt.cert_url

Definition at line 184 of file up_down.py.

10.172.3.2 rpki.up_down.class_elt.certs

Definition at line 170 of file up_down.py.

10.172.3.3 rpki.up_down.class_elt.class_name

Definition at line 183 of file up_down.py.

10.172.3.4 rpki.up_down.class_elt.issuer = None [static]

Definition at line 165 of file up_down.py.

10.172.3.5 rpki.up_down.class_elt.resource_set_as

Definition at line 186 of file up_down.py.

10.172.3.6 rpki.up_down.class_elt.resource_set_ipv4

Definition at line 187 of file up_down.py.

10.172.3.7 rpki.up_down.class_elt.resource_set_ipv6

Definition at line 188 of file up_down.py.

10.172.3.8 rpki.up_down.class_elt.resource_set_notafter

Definition at line 189 of file up_down.py.

10.172.3.9 rpki.up_down.class_elt.suggested_sia_head

Definition at line 185 of file up_down.py.

The documentation for this class was generated from the following file:

- [up_down.py \(2793\)](#)

10.173 rpki.up_down.class_response_syntax Class Reference

Inherits [rpki::up_down::base_elt](#).

Inherited by [rpki.up_down.issue_response_pdu](#), and [rpki.up_down.list_response_pdu](#).

Public Member Functions

- def [__init__](#)
- def [startElement](#)
- def [toXML](#)

Public Attributes

- [classes](#)

10.173.1 Detailed Description

Syntax for Up-Down protocol "list_response" and "issue_response" PDUs.

Definition at line 284 of file up_down.py.

10.173.2 Member Function Documentation

10.173.2.1 def rpki.up_down.class_response_syntax.__init__ (self)

Initialize `class_response_syntax`.

Definition at line 289 of file `up_down.py`.

10.173.2.2 **def rpki.up_down.class_response_syntax.startElement (*self*, *stack*, *name*, *attrs*)**

Handle "list_response" and "issue_response" PDUs.

Reimplemented from [rpki.up_down.base_elt](#).

Definition at line 296 of file `up_down.py`.

10.173.2.3 **def rpki.up_down.class_response_syntax.toXML (*self*)**

Generate payload of "list_response" and "issue_response" PDUs.

Definition at line 306 of file `up_down.py`.

10.173.3 Member Data Documentation

10.173.3.1 **rpki.up_down.class_response_syntax.classes**

Definition at line 294 of file `up_down.py`.

The documentation for this class was generated from the following file:

- [up_down.py \(2793\)](#)

10.174 **rpki.up_down.cms_msg Class Reference**

Inherits [rpki::x509::XML_CMS_object](#).

Inherited by [rootd.cms_msg](#).

Static Public Attributes

- string [encoding](#) = "UTF-8"
- [saxify](#) = sax_handler.saxify
- [schema](#) = rpki.relaxng.up_down

10.174.1 Detailed Description

Class to hold a CMS-signed up-down PDU.

Definition at line 683 of file up_down.py.

10.174.2 Member Data Documentation

10.174.2.1 string rpki.up_down.cms_msg.encoding = "UTF-8" [static]

Definition at line 688 of file up_down.py.

10.174.2.2 rpki.up_down.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented in [rootd.cms_msg](#).

Definition at line 690 of file up_down.py.

10.174.2.3 rpki.up_down.cms_msg.schema = rpki.relaxng.up_down [static]

Definition at line 689 of file up_down.py.

The documentation for this class was generated from the following file:

- [up_down.py \(2793\)](#)

10.175 rpki.up_down.error_response_pdu Class Reference

Inherits [rpki::up_down::base_elt](#).

Public Member Functions

- def [__init__](#)
- def [check_response](#)
- def [endElement](#)
- def [toXML](#)

Public Attributes

- [description](#)
- [status](#)

Static Public Attributes

- dictionary [codes](#)
- dictionary [exceptions](#)

10.175.1 Detailed Description

Up-Down protocol "error_response" PDU.

Definition at line 503 of file up_down.py.

10.175.2 Member Function Documentation

10.175.2.1 def rpki.up_down.error_response_pdu.__init__ (self, exception = None)

Initialize an error_response PDU from an exception object.

Definition at line 522 of file up_down.py.

10.175.2.2 def rpki.up_down.error_response_pdu.check_response (self)

Handle an error response. For now, just raise an exception, perhaps figure out something more clever to do later.

Reimplemented from [rpki.up_down.base_elt](#).

Definition at line 562 of file up_down.py.

10.175.2.3 def rpki.up_down.error_response_pdu.endElement (self, stack, name, text)

Handle "error_response" PDU.

Reimplemented from [rpki.up_down.base_elt](#).

Definition at line 531 of file up_down.py.

10.175.2.4 def rpki.up_down.error_response_pdu.toXML (self)

Generate payload of "error_response" PDU.

Definition at line 547 of file up_down.py.

10.175.3 Member Data Documentation

10.175.3.1 dictionary rpki.up_down.error_response_pdu.codes [static]

Initial value:

```
{
    1101 : "Already processing request",
    1102 : "Version number error",
    1103 : "Unrecognised request type",
    1201 : "Request - no such resource class",
    1202 : "Request - no resources allocated in resource class",
    1203 : "Request - badly formed certificate request",
    1301 : "Revoke - no such resource class",
    1302 : "Revoke - no such key",
    2001 : "Internal Server Error - Request not performed" }
```

Definition at line 508 of file up_down.py.

10.175.3.2 rpki.up_down.error_response_pdu.description

Definition at line 529 of file up_down.py.

10.175.3.3 dictionary `rpki.up_down.error_response_pdu.exceptions` [static]

Initial value:

```
{  
    rpki.exceptions.NoActiveCA : 1202 }
```

Definition at line 519 of file `up_down.py`.

10.175.3.4 `rpki.up_down.error_response_pdu.status`

Definition at line 528 of file `up_down.py`.

The documentation for this class was generated from the following file:

- [up_down.py \(2793\)](#)

10.176 rpki.up_down.issue_pdu Class Reference

Inherits [rpki::up_down::base_elt](#).

Inherited by [rootd.issue_pdu](#).

Public Member Functions

- def [endElement](#)
- def [query](#)
- def [serve_pdu](#)
- def [startElement](#)
- def [toXML](#)

Public Attributes

- [class_name](#)
- [pkcs10](#)
- [req_resource_set_as](#)
- [req_resource_set_ipv4](#)
- [req_resource_set_ipv6](#)

10.176.1 Detailed Description

Up-Down protocol "issue" PDU.

Definition at line 316 of file up_down.py.

10.176.2 Member Function Documentation

10.176.2.1 `def rpki.up_down.issue_pdu.endElement (self, stack, name, text)`

Handle "issue" PDU.

Reimplemented from [rpki.up_down.base_elt](#).

Definition at line 331 of file up_down.py.

10.176.2.2 `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 416 of file up_down.py.

10.176.2.3 `def rpki.up_down.issue_pdu.serve_pdu (self, q_msg, r_msg, child, callback, errback)`

Serve one issue request PDU.

Reimplemented from [rpki.up_down.base_elt](#).

Reimplemented in [rootd.issue_pdu](#).

Definition at line 348 of file up_down.py.

10.176.2.4 `def rpki.up_down.issue_pdu.startElement (self, stack, name, attrs)`

Handle "issue" PDU.

Reimplemented from [rpki.up_down.base_elt](#).

Definition at line 321 of file up_down.py.

10.176.2.5 def rpki.up_down.issue_pdu.toXML (*self*)

Generate payload of "issue" PDU.

Definition at line 339 of file up_down.py.

10.176.3 Member Data Documentation

10.176.3.1 rpki.up_down.issue_pdu.class_name

Definition at line 326 of file up_down.py.

10.176.3.2 rpki.up_down.issue_pdu.pkcs10

Definition at line 336 of file up_down.py.

10.176.3.3 rpki.up_down.issue_pdu.req_resource_set_as

Definition at line 327 of file up_down.py.

10.176.3.4 rpki.up_down.issue_pdu.req_resource_set_ipv4

Definition at line 328 of file up_down.py.

10.176.3.5 rpki.up_down.issue_pdu.req_resource_set_ipv6

Definition at line 329 of file up_down.py.

The documentation for this class was generated from the following file:

- [up_down.py \(2793\)](#)

10.177 rpki.up_down.issue_response_pdu Class Reference

Inherits [rpki::up_down::class_response_syntax](#).

Public Member Functions

- def [check_response](#)

10.177.1 Detailed Description

Up-Down protocol "issue_response" PDU.

Definition at line 428 of file up_down.py.

10.177.2 Member Function Documentation

10.177.2.1 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 433 of file up_down.py.

The documentation for this class was generated from the following file:

- [up_down.py \(2793\)](#)

10.178 rpki.up_down.list_pdu Class Reference

Inherits [rpki::up_down::base_elt](#).

Inherited by [rootd.list_pdu](#).

Public Member Functions

- def [query](#)
- def [serve_pdu](#)
- def [toXML](#)

10.178.1 Detailed Description

Up-Down protocol "list" PDU.

Definition at line 231 of file up_down.py.

10.178.2 Member Function Documentation

10.178.2.1 def rpki.up_down.list_pdu.query (*cls*, *parent*, *cb*, *eb*)

Send a "list" query to parent.

Definition at line 273 of file up_down.py.

10.178.2.2 def rpki.up_down.list_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*, *callback*, *errback*)

Serve one "list" PDU.

Reimplemented from [rpki.up_down.base_elt](#).

Reimplemented in [rootd.list_pdu](#).

Definition at line 240 of file up_down.py.

10.178.2.3 def rpki.up_down.list_pdu.toXML (*self*)

Generate (empty) payload of "list" PDU.

Definition at line 236 of file up_down.py.

The documentation for this class was generated from the following file:

- [up_down.py \(2793\)](#)

10.179 rpki.up_down.list_response_pdu Class Reference

Inherits [rpki::up_down::class_response_syntax](#).

10.179.1 Detailed Description

Up-Down protocol "list_response" PDU.

Definition at line 310 of file up_down.py.

The documentation for this class was generated from the following file:

- [up_down.py \(2793\)](#)

10.180 rpki.up_down.message_pdu Class Reference

Inherits [rpki::up_down::base_elt](#).

Inherited by [rootd.message_pdu](#).

Public Member Functions

- def [__str__](#)
- def [log_query](#)
- def [make_query](#)
- def [serve_error](#)
- def [serve_top_level](#)
- def [startElement](#)
- def [toXML](#)

Public Attributes

- [payload](#)
- [recipient](#)
- [sender](#)
- [type](#)
- [version](#)

Static Public Attributes

- dictionary [name2type](#)
- tuple [type2name](#) = dict((v, k) for k, v in name2type.items())
- int [version](#) = 1

10.180.1 Detailed Description

Up-Down protocol message wrapper PDU.

Definition at line 569 of file up_down.py.

10.180.2 Member Function Documentation

10.180.2.1 def rpki.up_down.message_pdu.__str__ (self)

Convert a message PDU to a string.

Definition at line 611 of file up_down.py.

10.180.2.2 def rpki.up_down.message_pdu.log_query (self, child)

Log query we're handling. Separate method so rootd can override.

Reimplemented in [rootd.message_pdu](#).

Definition at line 640 of file up_down.py.

10.180.2.3 def rpki.up_down.message_pdu.make_query (cls, payload, sender, recipient)

Construct one message PDU.

Definition at line 658 of file up_down.py.

10.180.2.4 def rpki.up_down.message_pdu.serve_error (self, exception)

Generate an error_response message PDU.

Definition at line 646 of file up_down.py.

10.180.2.5 `def rpki.up_down.message_pdu.serve_top_level (self, child, callback)`

Serve one message request PDU.

Definition at line 615 of file up_down.py.

10.180.2.6 `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 595 of file up_down.py.

10.180.2.7 `def rpki.up_down.message_pdu.toXML (self)`

Generate payload of message PDU.

Definition at line 587 of file up_down.py.

10.180.3 Member Data Documentation**10.180.3.1** dictionary `rpki.up_down.message_pdu.name2type` [static]

Initial value:

```
{
    "list" : list_pdu,
    "list_response" : list_response_pdu,
    "issue" : issue_pdu,
    "issue_response" : issue_response_pdu,
    "revoke" : revoke_pdu,
    "revoke_response" : revoke_response_pdu,
    "error_response" : error_response_pdu }
```

Reimplemented in [rootd.message_pdu](#).

Definition at line 576 of file up_down.py.

10.180.3.2 rpki.up_down.message_pdu.payload

Definition at line 608 of file up_down.py.

10.180.3.3 rpki.up_down.message_pdu.recipient

Definition at line 606 of file up_down.py.

10.180.3.4 rpki.up_down.message_pdu.sender

Definition at line 605 of file up_down.py.

10.180.3.5 rpki.up_down.message_pdu.type

Definition at line 607 of file up_down.py.

10.180.3.6 tuple rpki.up_down.message_pdu.type2name = dict((v, k) for k, v in name2type.items()) [static]

Reimplemented in [rootd.message_pdu](#).

Definition at line 585 of file up_down.py.

10.180.3.7 rpki.up_down.message_pdu.version

Definition at line 604 of file up_down.py.

10.180.3.8 int rpki.up_down.message_pdu.version = 1 [static]

Definition at line 574 of file up_down.py.

The documentation for this class was generated from the following file:

- [up_down.py \(2793\)](#)

10.181 rpki.up_down.multi_uri Class Reference

Inherits list.

Public Member Functions

- [def __init__](#)
- [def __str__](#)
- [def rsync](#)

10.181.1 Detailed Description

Container for a set of URIs.

Definition at line 95 of file up_down.py.

10.181.2 Member Function Documentation

10.181.2.1 def rpki.up_down.multi_uri.__init__ (self, ini)

Initialize a set of URIs, which includes basic some syntax checking.

Definition at line 100 of file up_down.py.

10.181.2.2 def rpki.up_down.multi_uri.__str__ (self)

Convert a multi_uri back to a string representation.

Definition at line 115 of file up_down.py.

10.181.2.3 def rpki.up_down.multi_uri.rsync (self)

Find first rsync://... URI in self.

Definition at line 119 of file up_down.py.

The documentation for this class was generated from the following file:

- [up_down.py \(2793\)](#)

10.182 rpki.up_down.revoke_pdu Class Reference

Inherits [rpki::up_down::revoke_syntax](#).

Inherited by [rootd.revoke_pdu](#).

Public Member Functions

- def [get_SKI](#)
- def [query](#)
- def [serve_pdu](#)

Public Attributes

- [class_name](#)
- [ski](#)

10.182.1 Detailed Description

Up-Down protocol "revoke" PDU.

Definition at line 455 of file up_down.py.

10.182.2 Member Function Documentation

10.182.2.1 def rpki.up_down.revoke_pdu.get_SKI (self)

Convert g(SKI) encoding from PDU back to raw SKI.

Definition at line 460 of file up_down.py.

10.182.2.2 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 486 of file up_down.py.

10.182.2.3 def rpki.up_down.revoke_pdu.serve_pdu (self, q_msg, r_msg, child, cb, eb)

Serve one revoke request PDU.

Reimplemented from [rpki.up_down.base_elt](#).

Reimplemented in [rootd.revoke_pdu](#).

Definition at line 464 of file up_down.py.

10.182.3 Member Data Documentation

10.182.3.1 rpki.up_down.revoke_pdu.class_name

Reimplemented from [rpki.up_down.revoke_syntax](#).

Definition at line 492 of file up_down.py.

10.182.3.2 rpki.up_down.revoke_pdu.ski

Reimplemented from [rpki.up_down.revoke_syntax](#).

Definition at line 493 of file up_down.py.

The documentation for this class was generated from the following file:

- [up_down.py \(2793\)](#)

10.183 rpki.up_down.revoke_response_pdu Class Reference

Inherits [rpki::up_down::revoke_syntax](#).

10.183.1 Detailed Description

Up-Down protocol "revoke_response" PDU.

Definition at line 496 of file up_down.py.

The documentation for this class was generated from the following file:

- [up_down.py \(2793\)](#)

10.184 rpki.up_down.revoke_syntax Class Reference

Inherits [rpki::up_down::base_elt](#).

Inherited by [rpki.up_down.revoke_pdu](#), and [rpki.up_down.revoke_response_pdu](#).

Public Member Functions

- def [startElement](#)
- def [toXML](#)

Public Attributes

- [class_name](#)
- [ski](#)

10.184.1 Detailed Description

Syntax for Up-Down protocol "revoke" and "revoke_response" PDUs.

Definition at line 441 of file up_down.py.

10.184.2 Member Function Documentation

10.184.2.1 def rpki.up_down.revoke_syntax.startElement (*self*, *stack*, *name*, *attrs*)

Handle "revoke" PDU.

Reimplemented from [rpki.up_down.base_elt](#).

Definition at line 446 of file up_down.py.

10.184.2.2 def rpki.up_down.revoke_syntax.toXML (*self*)

Generate payload of "revoke" PDU.

Definition at line 451 of file up_down.py.

10.184.3 Member Data Documentation

10.184.3.1 rpki.up_down.revoke_syntax.class_name

Reimplemented in [rpki.up_down.revoke_pdu](#).

Definition at line 448 of file up_down.py.

10.184.3.2 rpki.up_down.revoke_syntax.ski

Reimplemented in [rpki.up_down.revoke_pdu](#).

Definition at line 449 of file up_down.py.

The documentation for this class was generated from the following file:

- [up_down.py \(2793\)](#)

10.185 rpki.up_down.sax_handler Class Reference

Inherits [rpki.xml_utils.sax_handler](#).

Inherited by [rootd.sax_handler](#).

Static Public Attributes

- string [name](#) = "message"
- [pdu](#) = [message_pdu](#)
- string [version](#) = "1"

10.185.1 Detailed Description

SAX handler for Up-Down protocol.

Definition at line 674 of file up_down.py.

10.185.2 Member Data Documentation

10.185.2.1 string rpki.up_down.sax_handler.name = "message" [static]

Definition at line 680 of file up_down.py.

10.185.2.2 rpki.up_down.sax_handler.pdu = message_pdu [static]

Reimplemented in [rootd.sax_handler](#).

Definition at line 679 of file up_down.py.

10.185.2.3 string rpki.up_down.sax_handler.version = "1" [static]

Definition at line 681 of file up_down.py.

The documentation for this class was generated from the following file:

- [up_down.py \(2793\)](#)

10.186 rpki.x509.CMS_object Class Reference

Inherits [rpki::x509::DER_object](#).

Inherited by [rpki.x509.DER_CMS_object](#), and [rpki.x509.XML_CMS_object](#).

Public Member Functions

- def [extract](#)
- def [get_content](#)
- def [get_DER](#)
- def [get_POW](#)
- def [set_content](#)
- def [sign](#)
- def [verify](#)

Public Attributes

- `content`
- `DER`
DER value of this `object`.
- `POW`

Static Public Attributes

- `debug_cms_certs` = False
Set this to True to `log` a lot of chatter about CMS certificates.
- `dump_on_verify_failure` = True
Set this to True to get `dumpasn1` dumps of ASN.1 on CMS verify failures.
- tuple `econtent_oid` = `POWify_OID("id-data")`
- tuple `formats` = ("DER", "`POW`")
Formats supported in this `object`.
- tuple `other_clear` = ("content",)
Other attributes that `self.clear()` should whack.
- tuple `pem_converter` = `PEM_converter("CMS")`
PEM converter for this `object`.
- `print_on_der_error` = True
Set this to True to `log` alleged DER when we have trouble parsing it, in case it's really a Perl backtrace or something.
- `require_crls` = False
Set this to False to make CMS CRLs optional in the cases where we would otherwise require them.

10.186.1 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 701 of file x509.py.

10.186.2 Member Function Documentation

10.186.2.1 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 851 of file x509.py.

10.186.2.2 def rpki.x509.CMS_object.get_content (*self*)

Get the inner content of this CMS_object.

Definition at line 763 of file x509.py.

10.186.2.3 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 742 of file x509.py.

10.186.2.4 def rpki.x509.CMS_object.get_POW (*self*)

Get the POW value of this CMS_object.

Definition at line 754 of file x509.py.

10.186.2.5 def rpki.x509.CMS_object.set_content (self, content)

Set the (inner) content of this CMS_object, clearing the wrapper.

Definition at line 770 of file x509.py.

10.186.2.6 def rpki.x509.CMS_object.sign (self, keypair, certs, crls = None, no_certs = False)

Sign and wrap inner content.

Definition at line 879 of file x509.py.

10.186.2.7 def rpki.x509.CMS_object.verify (self, ta)

Verify CMS wrapper and store inner content.

Definition at line 777 of file x509.py.

10.186.3 Member Data Documentation**10.186.3.1 rpki.x509.CMS_object.content**

Reimplemented in [rpki.x509.DER_CMS_object](#), and [rpki.x509.XML_CMS_object](#).

Definition at line 775 of file x509.py.

10.186.3.2 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 727 of file x509.py.

10.186.3.3 rpki.x509.CMS_object.DER

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 750 of file x509.py.

10.186.3.4 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 722 of file x509.py.

10.186.3.5 tuple rpki.x509.CMS_object.econtent_oid = POWify_OID("id-data") [static]

Reimplemented in [rpki.x509.SignedManifest](#), [rpki.x509.ROA](#), and [rpki.x509.XML_CMS_object](#).

Definition at line 716 of file x509.py.

10.186.3.6 tuple rpki.x509.CMS_object.formats = ("DER", "POW") [static]

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 714 of file x509.py.

10.186.3.7 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 715 of file x509.py.

10.186.3.8 `tuple rpki.x509.CMS_object.pem_converter = PEM_converter("CMS") [static]`

PEM converter for this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Reimplemented in [rpki.x509.SignedManifest](#), and [rpki.x509.ROA](#).

Definition at line 717 of file x509.py.

10.186.3.9 `rpki.x509.CMS_object.POW`

Definition at line 760 of file x509.py.

10.186.3.10 `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 740 of file x509.py.

10.186.3.11 `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 734 of file x509.py.

The documentation for this class was generated from the following file:

- [x509.py \(2784\)](#)

10.187 rpki.x509.CRL Class Reference

Inherits [rpki::x509::DER_object](#).

Public Member Functions

- def [generate](#)
- def [get_DER](#)
- def [get_POW](#)
- def [get_POWpkix](#)
- def [getIssuer](#)
- def [getNextUpdate](#)
- def [getThisUpdate](#)

Public Attributes

- [DER](#)
DER value of this [object](#).
- [POW](#)
- [POWpkix](#)

Static Public Attributes

- tuple [formats](#) = ("DER", "POW", "POWpkix")
Formats supported in this [object](#).
- tuple [pem_converter](#) = [PEM_converter](#)("X509 CRL")
PEM converter for this [object](#).

10.187.1 Detailed Description

Class to hold a Certificate Revocation List.

Definition at line 1079 of file x509.py.

10.187.2 Member Function Documentation

10.187.2.1 `def rpki.x509.CRL.generate (cls, keypair, issuer, serial, thisUpdate, nextUpdate, revokedCertificates, version = 1, digestType = "sha256WithRSAEncryption")`

Generate a new CRL.

Definition at line 1135 of file x509.py.

10.187.2.2 def rpki.x509.CRL.get_DER (self)

Get the DER value of this CRL.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 1087 of file x509.py.

10.187.2.3 def rpki.x509.CRL.get_POW (self)

Get the POW value of this CRL.

Definition at line 1102 of file x509.py.

10.187.2.4 def rpki.x509.CRL.get_POWpkix (self)

Get the POW.pkix value of this CRL.

Definition at line 1111 of file x509.py.

10.187.2.5 def rpki.x509.CRL.getIssuer (self)

Get issuer value of this CRL.

Definition at line 1130 of file x509.py.

10.187.2.6 def rpki.x509.CRL.getNextUpdate (self)

Get nextUpdate value from this CRL.

Definition at line 1126 of file x509.py.

10.187.2.7 def rpki.x509.CRL.getThisUpdate (self)

Get thisUpdate value from this CRL.

Definition at line 1122 of file x509.py.

10.187.3 Member Data Documentation

10.187.3.1 rpki.x509.CRL.DER

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 1095 of file x509.py.

10.187.3.2 tuple rpki.x509.CRL.formats = ("DER", "POW", "POWpkix") [static]

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 1084 of file x509.py.

10.187.3.3 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 1085 of file x509.py.

10.187.3.4 rpki.x509.CRL.POW

Definition at line 1108 of file x509.py.

10.187.3.5 rpki.x509.CRL.POWpkix

Definition at line 1119 of file x509.py.

The documentation for this class was generated from the following file:

- [x509.py \(2784\)](#)

10.188 rpki.x509.DER_CMS_object Class Reference

Inherits [rpki::x509::CMS_object](#).

Inherited by [rpki.x509.ROA](#), and [rpki.x509.SignedManifest](#).

Public Member Functions

- def [decode](#)
- def [encode](#)

Public Attributes

- [content](#)

10.188.1 Detailed Description

Class to hold CMS objects with DER-based content.

Definition at line 915 of file x509.py.

10.188.2 Member Function Documentation

10.188.2.1 def rpki.x509.DER_CMS_object.decode (self, der)

Decode DER and set inner content.

Definition at line 924 of file x509.py.

10.188.2.2 def rpki.x509.DER_CMS_object.encode (self)

Encode inner content for signing.

Definition at line 920 of file x509.py.

10.188.3 Member Data Documentation

10.188.3.1 rpki.x509.DER_CMS_object.content

Reimplemented from [rpki.x509.CMS_object](#).

Definition at line 930 of file x509.py.

The documentation for this class was generated from the following file:

- [x509.py \(2784\)](#)

10.189 rpki.x509.DER_object Class Reference

Inherits [object](#).

Inherited by [rpki.x509.CMS_object](#), [rpki.x509.CRL](#), [rpki.x509.PKCS10](#), [rpki.x509.RSA](#), [rpki.x509.RSAPublic](#), and [rpki.x509.X509](#).

Public Member Functions

- def [__cmp__](#)
- def [__init__](#)
- def [clear](#)
- def [dumpasn1](#)
- def [empty](#)
- def [from_sql](#)
- def [gAKI](#)
- def [get_3779resources](#)
- def [get_AIA](#)
- def [get_AKI](#)
- def [get_Base64](#)
- def [get_basicConstraints](#)
- def [get_DER](#)

- def [get_PEM](#)
- def [get_SIA](#)
- def [get_SKI](#)
- def [gSKI](#)
- def [hAKI](#)
- def [hSKI](#)
- def [is_CA](#)
- def [set](#)
- def [to_sql](#)

Public Attributes

- [DER](#)
DER value of this [object](#).

Static Public Attributes

- tuple [formats](#) = ("DER",)
Formats supported in this [object](#).
- tuple [other_clear](#) = ()
Other attributes that [self.clear\(\)](#) should whack.
- [pem_converter](#) = None
PEM converter for this [object](#).

10.189.1 Detailed Description

Virtual class to hold a generic DER object.

Definition at line 104 of file x509.py.

10.189.2 Member Function Documentation

10.189.2.1 def rpki.x509.DER_object.__cmp__ (*self*, *other*)

Compare two DER-encoded objects.

Definition at line 199 of file x509.py.

10.189.2.2 def rpki.x509.DER_object.__init__ (self, kw)

Initialize a DER_object.

Definition at line 137 of file x509.py.

10.189.2.3 def rpki.x509.DER_object.clear (self)

Make this object empty.

Definition at line 130 of file x509.py.

10.189.2.4 def rpki.x509.DER_object.dumpasn1 (self)

Pretty print an ASN.1 DER object using cryptlib dumpasn1 tool.
Use a temporary file rather than popen4() because dumpasn1 uses
seek() when decoding ASN.1 content nested in OCTET STRING values.

Definition at line 307 of file x509.py.

10.189.2.5 def rpki.x509.DER_object.empty (self)

Test whether this object is empty.

Definition at line 121 of file x509.py.

10.189.2.6 def rpki.x509.DER_object.from_sql (cls, x)

Convert from SQL storage format.

Definition at line 299 of file x509.py.

10.189.2.7 def rpki.x509.DER_object.gAKI (self)

Calculate g(AKI) for this object. Only work for subclasses that implement get_AKI().

Definition at line 235 of file x509.py.

10.189.2.8 def rpki.x509.DER_object.get_3779resources (self)

Get RFC 3779 resources as rpki.resource_set objects. Only works for subclasses that support getExtensions().

Definition at line 286 of file x509.py.

10.189.2.9 def rpki.x509.DER_object.get_AIA (self)

Get the SIA extension from this object. Only works for subclasses that support getExtension().

Definition at line 264 of file x509.py.

10.189.2.10 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 242 of file x509.py.

10.189.2.11 def rpki.x509.DER_object.get_Base64 (self)

Get the Base64 encoding of the DER value of this object.

Definition at line 191 of file x509.py.

10.189.2.12 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 271 of file x509.py.

10.189.2.13 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 180 of file x509.py.

10.189.2.14 def rpki.x509.DER_object.get_PEM (self)

Get the PEM representation of this object.

Definition at line 195 of file x509.py.

10.189.2.15 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 257 of file x509.py.

10.189.2.16 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 250 of file `x509.py`.

10.189.2.17 def rpki.x509.DER_object.gSKI (self)

Calculate `g(SKI)` for this object. Only work for subclasses that implement `get_SKI()`.

Definition at line 220 of file `x509.py`.

10.189.2.18 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 227 of file `x509.py`.

10.189.2.19 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 212 of file `x509.py`.

10.189.2.20 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 278 of file `x509.py`.

10.189.2.21 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 145 of file x509.py.

10.189.2.22 def rpki.x509.DER_object.to_sql (self)

Convert to SQL storage format.

Definition at line 303 of file x509.py.

10.189.3 Member Data Documentation**10.189.3.1 rpki::x509.DER_object::DER**

DER value of this [object](#).

Reimplemented in [rpki.x509.X509](#), [rpki.x509.PKCS10](#), [rpki.x509.RSA](#), [rpki.x509.RSAPublic](#), [rpki.x509.CMS_object](#), and [rpki.x509.CRL](#).

Definition at line 163 of file x509.py.

10.189.3.2 tuple rpki.x509.DER_object.formats = ("DER",) [static]

Formats supported in this [object](#).

Reimplemented in [rpki.x509.X509](#), [rpki.x509.PKCS10](#), [rpki.x509.RSA](#), [rpki.x509.RSAPublic](#), [rpki.x509.CMS_object](#), and [rpki.x509.CRL](#).

Definition at line 110 of file x509.py.

10.189.3.3 tuple `rpki.x509.DER_object.other_clear = ()` [static]

Other attributes that `self.clear()` should whack.

Reimplemented in [rpki.x509.CMS_object](#).

Definition at line 116 of file `x509.py`.

10.189.3.4 `rpki.x509.DER_object.pem_converter = None` [static]

PEM converter for this [object](#).

Reimplemented in [rpki.x509.X509](#), [rpki.x509.PKCS10](#), [rpki.x509.RSA](#), [rpki.x509.RSAPublic](#), [rpki.x509.CMS_object](#), [rpki.x509.SignedManifest](#), [rpki.x509.ROA](#), and [rpki.x509.CRL](#).

Definition at line 113 of file `x509.py`.

The documentation for this class was generated from the following file:

- [x509.py](#) (2784)

10.190 rpki.x509.PEM_converter Class Reference

Inherits [object](#).

Public Member Functions

- `def __init__`
- `def looks_like_PEM`
- `def to_DER`
- `def to_PEM`

Public Attributes

- [b](#)
- [e](#)

10.190.1 Detailed Description

Convert between DER and PEM encodings for various kinds of ASN.1 data.

Definition at line 61 of file `x509.py`.

10.190.2 Member Function Documentation

10.190.2.1 def rpki.x509.PEM_converter.__init__ (*self*, *kind*)

Initialize PEM_converter.

Definition at line 66 of file x509.py.

10.190.2.2 def rpki.x509.PEM_converter.looks_like_PEM (*self*, *text*)

Guess whether text looks like a PEM encoding.

Definition at line 73 of file x509.py.

10.190.2.3 def rpki.x509.PEM_converter.to_DER (*self*, *pem*)

Convert from PEM to DER.

Definition at line 80 of file x509.py.

10.190.2.4 def rpki.x509.PEM_converter.to_PEM (*self*, *der*)

Convert from DER to PEM.

Definition at line 93 of file x509.py.

10.190.3 Member Data Documentation

10.190.3.1 rpki.x509.PEM_converter.b

Definition at line 70 of file x509.py.

10.190.3.2 rpki.x509.PEM_converter.e

Definition at line 71 of file x509.py.

The documentation for this class was generated from the following file:

- [x509.py \(2784\)](#)

10.191 rpki.x509.PKCS10 Class Reference

Inherits [rpki::x509::DER_object](#).

Public Member Functions

- def [check_valid_rpki](#)
- def [create](#)
- def [create_ca](#)
- def [get_DER](#)
- def [get_POWpkix](#)
- def [getPublicKey](#)

Public Attributes

- [DER](#)
DER value of this [object](#).
- [POWpkix](#)

Static Public Attributes

- tuple [formats](#) = ("DER", "[POWpkix](#)")
Formats supported in this [object](#).
- tuple [pem_converter](#) = [PEM_converter](#)("CERTIFICATE REQUEST")
PEM converter for this [object](#).

10.191.1 Detailed Description

Class to hold a PKCS #10 request.

Definition at line 500 of file x509.py.

10.191.2 Member Function Documentation

10.191.2.1 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 535 of file x509.py.

10.191.2.2 def rpki.x509.PKCS10.create (cls, keypair, exts = None)

Create a new request for a given keypair, including given extensions.

Definition at line 595 of file x509.py.

10.191.2.3 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 582 of file x509.py.

10.191.2.4 def rpki.x509.PKCS10.get_DER (self)

Get the DER value of this certification request.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 508 of file x509.py.

10.191.2.5 def rpki.x509.PKCS10.get_POWpkix (self)

Get the POW.pkix value of this certification request.

Definition at line 520 of file x509.py.

10.191.2.6 def rpki.x509.PKCS10.getPublicKey (self)

Extract the public key from this certification request.

Definition at line 531 of file x509.py.

10.191.3 Member Data Documentation**10.191.3.1 rpki.x509.PKCS10.DER**

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 516 of file x509.py.

**10.191.3.2 tuple rpki.x509.PKCS10.formats = ("DER", "POWpkix")
[static]**

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 505 of file x509.py.

**10.191.3.3 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 506 of file x509.py.

10.191.3.4 rpki.x509.PKCS10.POWpkix

Definition at line 528 of file x509.py.

The documentation for this class was generated from the following file:

- [x509.py \(2784\)](#)

10.192 rpki.x509.ROA Class Reference

Inherits [rpki::x509::DER_CMS_object](#).

Public Member Functions

- def [build](#)

Static Public Attributes

- [content_class](#) = [rpki.roa.RouteOriginAttestation](#)
- tuple [econtent_oid](#) = [POWify_OID](#)("id-ct-routeOriginAttestation")
- tuple [pem_converter](#) = [PEM_converter](#)("ROUTE ORIGIN ATTESTATION")
PEM converter for this [object](#).

10.192.1 Detailed Description

Class to hold a signed ROA.

Definition at line 972 of file x509.py.

10.192.2 Member Function Documentation

10.192.2.1 def rpki.x509.ROA.build (*cls*, *asn*, *ipv4*, *ipv6*, *keypair*, *certs*, *version* = 0)

Build a ROA.

Definition at line 982 of file x509.py.

10.192.3 Member Data Documentation

10.192.3.1 `rpki.x509.ROA.content_class = rpki.roa.RouteOriginAttestation` [static]

Definition at line 978 of file x509.py.

10.192.3.2 `tuple rpki.x509.ROA.econtent_oid = POWify_OID("id-ct-routeOriginAttestation")` [static]

Reimplemented from [rpki.x509.CMS_object](#).

Definition at line 979 of file x509.py.

10.192.3.3 `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 977 of file x509.py.

The documentation for this class was generated from the following file:

- [x509.py \(2784\)](#)

10.193 rpki.x509.RSA Class Reference

Inherits [rpki::x509::DER_object](#).

Public Member Functions

- def [generate](#)
- def [get_DER](#)
- def [get_POW](#)
- def [get_public_DER](#)
- def [get_RSAPublic](#)
- def [get_SKI](#)

Public Attributes

- [DER](#)

DER value of this [object](#).

- [POW](#)

Static Public Attributes

- tuple [formats](#) = ("DER", "[POW](#)")

Formats supported in this [object](#).

- tuple [pem_converter](#) = [PEM_converter](#)("RSA PRIVATE KEY")

PEM converter for this [object](#).

10.193.1 Detailed Description

Class to hold an RSA key pair.

Definition at line 609 of file x509.py.

10.193.2 Member Function Documentation

10.193.2.1 def rpki.x509.RSA.generate (cls, keylength = 2048)

Generate a new keypair.

Definition at line 639 of file x509.py.

10.193.2.2 def rpki.x509.RSA.get_DER (self)

Get the DER value of this keypair.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 617 of file x509.py.

10.193.2.3 def rpki.x509.RSA.get_POW (self)

Get the POW value of this keypair.

Definition at line 629 of file x509.py.

10.193.2.4 def rpki.x509.RSA.get_public_DER (self)

Get the DER encoding of the public key from this keypair.

Definition at line 646 of file x509.py.

10.193.2.5 def rpki.x509.RSA.get_RSAPublic (self)

Convert the public key of this keypair into a RSAPublic object.

Definition at line 654 of file x509.py.

10.193.2.6 def rpki.x509.RSA.get_SKI (self)

Calculate the SKI of this keypair.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 650 of file x509.py.

10.193.3 Member Data Documentation**10.193.3.1 rpki.x509.RSA.DER**

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 625 of file x509.py.

10.193.3.2 tuple rpki.x509.RSA.formats = ("DER", "POW") [static]

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 614 of file x509.py.

10.193.3.3 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 615 of file x509.py.

10.193.3.4 rpki.x509.RSA.POW

Definition at line 635 of file x509.py.

The documentation for this class was generated from the following file:

- [x509.py \(2784\)](#)

10.194 rpki.x509.RSAPublic Class Reference

Inherits [rpki::x509::DER_object](#).

Public Member Functions

- def [get_DER](#)
- def [get_POW](#)
- def [get_SKI](#)

Public Attributes

- [DER](#)
DER value of this [object](#).
- [POW](#)

Static Public Attributes

- tuple `formats` = ("DER", "POW")
Formats supported in this [object](#).
- tuple `pem_converter` = `PEM_converter`("RSA PUBLIC KEY")
PEM converter for this [object](#).

10.194.1 Detailed Description

Class to hold an RSA public key.

Definition at line 658 of file x509.py.

10.194.2 Member Function Documentation

10.194.2.1 `def rpki.x509.RSAPublic.get_DER (self)`

Get the DER value of this public key.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 666 of file x509.py.

10.194.2.2 `def rpki.x509.RSAPublic.get_POW (self)`

Get the POW value of this public key.

Definition at line 678 of file x509.py.

10.194.2.3 `def rpki.x509.RSAPublic.get_SKI (self)`

Calculate the SKI of this public key.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 687 of file x509.py.

10.194.3 Member Data Documentation

10.194.3.1 rpki.x509.RSAPublic.DER

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 674 of file x509.py.

10.194.3.2 tuple rpki.x509.RSAPublic.formats = ("DER", "POW") [static]

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 663 of file x509.py.

10.194.3.3 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 664 of file x509.py.

10.194.3.4 rpki.x509.RSAPublic.POW

Definition at line 684 of file x509.py.

The documentation for this class was generated from the following file:

- [x509.py \(2784\)](#)

10.195 rpki.x509.SignedManifest Class Reference

Inherits [rpki::x509::DER_CMS_object](#).

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](#).

10.195.1 Detailed Description

Class to hold a signed manifest.

Definition at line 932 of file x509.py.

10.195.2 Member Function Documentation

10.195.2.1 def rpki.x509.SignedManifest.build (cls, serial, thisUpdate, nextUpdate, names_and_objs, keypair, certs, version = 0)

Build a signed manifest.

Definition at line 950 of file x509.py.

10.195.2.2 def rpki.x509.SignedManifest.getNextUpdate (self)

Get nextUpdate value from this manifest.

Definition at line 945 of file x509.py.

10.195.2.3 `def rpki.x509.SignedManifest.getThisUpdate (self)`

Get thisUpdate value from this manifest.

Definition at line 941 of file x509.py.

10.195.3 Member Data Documentation**10.195.3.1** `rpki.x509.SignedManifest.content_class = rpki.manifest.Manifest
[static]`

Definition at line 938 of file x509.py.

10.195.3.2 `tuple rpki.x509.SignedManifest.econtent_oid =
POWify_OID("id-ct-rpkiManifest") [static]`

Reimplemented from [rpki.x509.CMS_object](#).

Definition at line 939 of file x509.py.

10.195.3.3 `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 937 of file x509.py.

The documentation for this class was generated from the following file:

- [x509.py \(2784\)](#)

10.196 rpki.x509.X509 Class Reference

Inherits [rpki::x509::DER_object](#).

Public Member Functions

- def [cross_certify](#)
- def [expired](#)
- def [get_DER](#)
- def [get_POW](#)
- def [get_POWpkix](#)
- def [getIssuer](#)
- def [getNotAfter](#)
- def [getNotBefore](#)
- def [getPublicKey](#)
- def [getSerial](#)
- def [getSubject](#)
- def [issue](#)
- def [normalize_chain](#)

Public Attributes

- [DER](#)
DER value of this [object](#).
- [POW](#)
- [POWpkix](#)

Static Public Attributes

- tuple [formats](#) = ("DER", "[POW](#)", "[POWpkix](#)")
Formats supported in this [object](#).
- tuple [pem_converter](#) = [PEM_converter](#)("CERTIFICATE")
PEM converter for this [object](#).

10.196.1 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 326 of file `x509.py`.

10.196.2 Member Function Documentation

10.196.2.1 `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 458 of file x509.py.

10.196.2.2 `def rpki.x509.X509.expired (self)`

Test whether this certificate has expired.

Definition at line 399 of file x509.py.

10.196.2.3 `def rpki.x509.X509.get_DER (self)`

Get the DER value of this certificate.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 340 of file x509.py.

10.196.2.4 `def rpki.x509.X509.get_POW (self)`

Get the POW value of this certificate.

Definition at line 355 of file x509.py.

10.196.2.5 `def rpki.x509.X509.get_POWpkix (self)`

Get the POW.pkix value of this certificate.

Definition at line 364 of file x509.py.

10.196.2.6 def rpki.x509.X509.getIssuer (*self*)

Get the issuer of this certificate.

Definition at line 375 of file x509.py.

10.196.2.7 def rpki.x509.X509.getNotAfter (*self*)

Get the expiration time of this certificate.

Definition at line 387 of file x509.py.

10.196.2.8 def rpki.x509.X509.getNotBefore (*self*)

Get the inception time of this certificate.

Definition at line 383 of file x509.py.

10.196.2.9 def rpki.x509.X509.getPublicKey (*self*)

Extract the public key from this certificate.

Definition at line 395 of file x509.py.

10.196.2.10 def rpki.x509.X509.getSerial (*self*)

Get the serial number of this certificate.

Definition at line 391 of file x509.py.

10.196.2.11 def rpki.x509.X509.getSubject (self)

Get the subject of this certificate.

Definition at line 379 of file x509.py.

10.196.2.12 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 403 of file x509.py.

10.196.2.13 def rpki.x509.X509.normalize_chain (cls, chain)

Normalize a chain of certificates into a tuple of X509 objects. Given all the glue certificates needed for BPKI cross certification, it's easiest to allow sloppy arguments to the HTTPS and CMS validation methods and provide a single method that normalizes the allowed cases. So this method allows X509, None, lists, and tuples, and returns a tuple of X509 objects.

Definition at line 487 of file x509.py.

10.196.3 Member Data Documentation**10.196.3.1 rpki.x509.X509.DER**

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 348 of file x509.py.

10.196.3.2 tuple `rpki.x509.X509.formats = ("DER", "POW", "POWpkix")`
[static]

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 337 of file `x509.py`.

10.196.3.3 tuple `rpki.x509.X509.pem_converter =`
`PEM_converter("CERTIFICATE")` [static]

PEM converter for this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 338 of file `x509.py`.

10.196.3.4 `rpki.x509.X509.POW`

Definition at line 361 of file `x509.py`.

10.196.3.5 `rpki.x509.X509.POWpkix`

Definition at line 372 of file `x509.py`.

The documentation for this class was generated from the following file:

- [x509.py \(2784\)](#)

10.197 rpki.x509.XML_CMS_object Class Reference

Inherits [rpki::x509::CMS_object](#).

Inherited by [rpki.left_right.cms_msg](#), [rpki.publication.cms_msg](#), and [rpki.up_down.cms_msg](#).

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
- [dump_outbound_cms](#) = None
 - If set, we write all outbound XML-CMS PDUs to disk, for debugging.*
- tuple [econtent_oid](#) = POWify_OID("id-ct-xml")

10.197.1 Detailed Description

Class to hold CMS-wrapped XML protocol data.

Definition at line 995 of file x509.py.

10.197.2 Member Function Documentation

10.197.2.1 def rpki.x509.XML_CMS_object.decode (self, xml)

Decode XML and set inner content.

Definition at line 1020 of file x509.py.

10.197.2.2 def rpki.x509.XML_CMS_object.dump_to_disk (self, prefix)

Write DER of current message to disk, for debugging.

Definition at line 1038 of file x509.py.

10.197.2.3 `def rpki.x509.XML_CMS_object.encode (self)`

Encode inner content for signing.

Definition at line 1016 of file x509.py.

10.197.2.4 `def rpki.x509.XML_CMS_object.pretty_print_content (self)`

Pretty print XML content of this message.

Definition at line 1024 of file x509.py.

10.197.2.5 `def rpki.x509.XML_CMS_object.schema_check (self)`

Handle XML RelaxNG schema check.

Definition at line 1028 of file x509.py.

10.197.2.6 `def rpki.x509.XML_CMS_object.unwrap (cls, der, ta, pretty_print = False)`

Unwrap a CMS-wrapped XML PDU and return Python objects.

Definition at line 1064 of file x509.py.

10.197.2.7 `def rpki.x509.XML_CMS_object.wrap (cls, msg, keypair, certs, crls = None, pretty_print = False)`

Build a CMS-wrapped XML PDU and return its DER encoding.

Definition at line 1047 of file x509.py.

10.197.3 Member Data Documentation

10.197.3.1 rpki.x509.XML_CMS_object.content

Reimplemented from [rpki.x509.CMS_object](#).

Definition at line 1022 of file x509.py.

10.197.3.2 rpki.x509.XML_CMS_object.dump_inbound_cms = None [static]

Definition at line 1014 of file x509.py.

10.197.3.3 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, we write all inbound XML-CMS PDUs to disk, for debugging.

Value of this variable is prefix portion of filename, tail will be a timestamp.

Definition at line 1007 of file x509.py.

10.197.3.4 tuple rpki.x509.XML_CMS_object.econtent_oid = POWify_OID("id-ct-xml") [static]

Reimplemented from [rpki.x509.CMS_object](#).

Definition at line 1000 of file x509.py.

The documentation for this class was generated from the following file:

- [x509.py \(2784\)](#)

10.198 rpki.xml_utils.base_elt Class Reference

Inherits [object](#).

Inherited by [rpki.left_right.list_resources_elt](#), [rpki.left_right.list_roa_requests_elt](#), [rpki.publication.publication_object_elt](#), [rpki.xml_utils.data_elt](#), and [rpki.xml_utils.text_elt](#).

Public Member Functions

- def [__str__](#)
- def [endElement](#)
- def [make_b64elt](#)
- def [make_elt](#)
- def [make_pdu](#)
- def [read_attrs](#)
- def [startElement](#)
- def [toXML](#)

Static Public Attributes

- tuple [attributes](#) = ()
XML attributes for this element.
- tuple [booleans](#) = ()
Boolean attributes (value "yes" or "no") for this element.
- tuple [elements](#) = ()
XML elements contained by this element.

10.198.1 Detailed Description

Virtual base class for XML message elements. The left-right and publication protocols use this. At least for now, the up-down protocol does not, due to different design assumptions.

Definition at line 126 of file `xml_utils.py`.

10.198.2 Member Function Documentation

10.198.2.1 def `rpki.xml_utils.base_elt.__str__ (self)`

Convert a `base_elt` object to string format.

Reimplemented in [rpki.publication.report_error_elt](#).

Definition at line 201 of file xml_utils.py.

10.198.2.2 def rpki.xml_utils.base_elt.endElement (self, stack, name, text)

Default endElement() handler: just pop the stack.

Reimplemented in [rpki.left_right.child_elt](#), [rpki.publication.client_elt](#), [rpki.publication.publication_object_elt](#), [rpki.xml_utils.text_elt](#), and [rpki.xml_utils.data_elt](#).

Definition at line 153 of file xml_utils.py.

10.198.2.3 def rpki.xml_utils.base_elt.make_b64elt (self, elt, name, value = None)

Constructor for Base64-encoded subelement.

Definition at line 192 of file xml_utils.py.

10.198.2.4 def rpki.xml_utils.base_elt.make_elt (self)

XML element constructor.

Definition at line 178 of file xml_utils.py.

10.198.2.5 def rpki.xml_utils.base_elt.make_pdu (cls, kargs)

Generic PDU constructor.

Definition at line 208 of file xml_utils.py.

10.198.2.6 `def rpki.xml_utils.base_elt.read_attrs (self, attrs)`

Template-driven attribute reader.

Definition at line 166 of file xml_utils.py.

10.198.2.7 `def rpki.xml_utils.base_elt.startElement (self, stack, name, attrs)`

Default startElement() handler: just process attributes.

Reimplemented in [rpki.left_right.list_resources_elt](#), [rpki.left_right.list_roa_requests_elt](#), and [rpki.publication.config_elt](#).

Definition at line 145 of file xml_utils.py.

10.198.2.8 `def rpki.xml_utils.base_elt.toXML (self)`

Default toXML() element generator.

Reimplemented in [rpki.left_right.list_resources_elt](#), [rpki.publication.publication_object_elt](#), [rpki.xml_utils.text_elt](#), and [rpki.xml_utils.data_elt](#).

Definition at line 160 of file xml_utils.py.

10.198.3 Member Data Documentation**10.198.3.1** `rpki::xml_utils.base_elt::attributes = ()` [static]

XML attributes for this element.

Reimplemented in [rpki.left_right.self_elt](#), [rpki.left_right.bsc_elt](#), [rpki.left_right.repository_elt](#), [rpki.left_right.parent_elt](#), [rpki.left_right.child_elt](#), [rpki.left_right.list_resources_elt](#), [rpki.left_right.list_roa_requests_elt](#), [rpki.left_right.list_published_objects_elt](#), [rpki.left_right.report_error_elt](#), [rpki.publication.config_elt](#), [rpki.publication.client_elt](#), [rpki.publication.publication_object_elt](#), and [rpki.publication.report_error_elt](#).

Definition at line 135 of file xml_utils.py.

10.198.3.2 rpki::xml_utils.base_elt::booleans = () [static]

Boolean attributes (value "yes" or "no") for this element.

Reimplemented in [rpki.left_right.self_elt](#), [rpki.left_right.bsc_elt](#), [rpki.left_right.parent_elt](#), and [rpki.left_right.child_elt](#).

Definition at line 143 of file [xml_utils.py](#).

10.198.3.3 rpki::xml_utils.base_elt::elements = () [static]

XML elements contained by this element.

Reimplemented in [rpki.left_right.self_elt](#), [rpki.left_right.bsc_elt](#), [rpki.left_right.repository_elt](#), [rpki.left_right.parent_elt](#), [rpki.left_right.child_elt](#), [rpki.publication.config_elt](#), and [rpki.publication.client_elt](#).

Definition at line 139 of file [xml_utils.py](#).

The documentation for this class was generated from the following file:

- [xml_utils.py](#) (2791)

10.199 rpki.xml_utils.data_elt Class Reference

Inherits [rpki::xml_utils::base_elt](#).

Inherited by [rpki.left_right.data_elt](#), and [rpki.publication.control_elt](#).

Public Member Functions

- def [endElement](#)
- def [make_reply](#)
- def [make_reply_clone_hook](#)
- def [serve_create](#)
- def [serve_destroy](#)
- def [serve_destroy_hook](#)
- def [serve_dispatch](#)
- def [serve_fetch_one](#)
- def [serve_get](#)
- def [serve_list](#)
- def [serve_post_save_hook](#)
- def [serve_pre_save_hook](#)

- def [serve_set](#)
- def [toXML](#)
- def [unimplemented_control](#)

10.199.1 Detailed Description

Virtual base class for PDUs that map to SQL objects. These objects all implement the create/set/get/list/destroy action attribute.

Definition at line 243 of file xml_utils.py.

10.199.2 Member Function Documentation

10.199.2.1 def rpki.xml_utils.data_elt.endElement (*self*, *stack*, *name*, *text*)

Default endElement handler for SQL-based objects. This assumes that sub-elements are Base64-encoded using the sql_template mechanism.

Reimplemented from [rpki.xml_utils.base_elt](#).

Reimplemented in [rpki.left_right.child_elt](#), and [rpki.publication.client_elt](#).

Definition at line 249 of file xml_utils.py.

10.199.2.2 def rpki.xml_utils.data_elt.make_reply (*self*, *r_pdu* = None)

Construct a reply PDU.

Definition at line 275 of file xml_utils.py.

10.199.2.3 def rpki.xml_utils.data_elt.make_reply_clone_hook (*self*, *r_pdu*)

Overridable hook.

Reimplemented in [rpki.left_right.data_elt](#).

Definition at line 292 of file xml_utils.py.

10.199.2.4 def rpki.xml_utils.data_elt.serve_create (self, r_msg, cb, eb)

Handle a create action.

Definition at line 314 of file xml_utils.py.

10.199.2.5 def rpki.xml_utils.data_elt.serve_destroy (self, r_msg, cb, eb)

Handle a destroy action.

Definition at line 384 of file xml_utils.py.

10.199.2.6 def rpki.xml_utils.data_elt.serve_destroy_hook (self, cb, eb)

Overridable hook.

Reimplemented in [rpki.left_right.child_elt](#).

Definition at line 378 of file xml_utils.py.

10.199.2.7 def rpki.xml_utils.data_elt.serve_dispatch (self, r_msg, cb, eb)

Action dispatch handler.

Reimplemented in [rpki.publication.control_elt](#).

Definition at line 395 of file xml_utils.py.

10.199.2.8 def rpki.xml_utils.data_elt.serve_fetch_one (self)

Find the object on which a get, set, or destroy method should operate.

Definition at line 296 of file xml_utils.py.

10.199.2.9 `def rpki.xml_utils.data_elt.serve_get (self, r_msg, cb, eb)`

Handle a get action.

Definition at line 360 of file xml_utils.py.

10.199.2.10 `def rpki.xml_utils.data_elt.serve_list (self, r_msg, cb, eb)`

Handle a list action for non-self objects.

Definition at line 369 of file xml_utils.py.

10.199.2.11 `def rpki.xml_utils.data_elt.serve_post_save_hook (self, q_pdu, r_pdu, cb, eb)`

Overridable hook.

Reimplemented in [rpki.left_right.self_elt](#), [rpki.left_right.parent_elt](#), [rpki.left_right.child_elt](#), and [rpki.publication.client_elt](#).

Definition at line 310 of file xml_utils.py.

10.199.2.12 `def rpki.xml_utils.data_elt.serve_pre_save_hook (self, q_pdu, r_pdu, cb, eb)`

Overridable hook.

Reimplemented in [rpki.left_right.data_elt](#), and [rpki.left_right.bsc_elt](#).

Definition at line 306 of file xml_utils.py.

10.199.2.13 `def rpki.xml_utils.data_elt.serve_set (self, r_msg, cb, eb)`

Handle a set action.

Reimplemented in [rpki.publication.config_elt](#).

Definition at line 337 of file xml_utils.py.

10.199.2.14 def rpki.xml_utils.data_elt.toXML (self)

Default element generator for SQL-based objects. This assumes that sub-elements are Base64-encoded DER objects.

Reimplemented from [rpki.xml_utils.base_elt](#).

Definition at line 263 of file xml_utils.py.

10.199.2.15 def rpki.xml_utils.data_elt.unimplemented_control (self, controls)

Uniform handling for unimplemented control operations.

Definition at line 408 of file xml_utils.py.

The documentation for this class was generated from the following file:

- [xml_utils.py \(2791\)](#)

10.200 rpki.xml_utils.msg Class Reference

Inherits list.

Inherited by [rpki.left_right.msg](#), and [rpki.publication.msg](#).

Public Member Functions

- def [__str__](#)
- def [endElement](#)
- def [is_query](#)
- def [is_reply](#)
- def [query](#)
- def [reply](#)
- def [startElement](#)
- def [toXML](#)

Public Attributes

- [type](#)
- [version](#)

10.200.1 Detailed Description

Generic top-level PDU.

Definition at line 416 of file xml_utils.py.

10.200.2 Member Function Documentation

10.200.2.1 def rpki.xml_utils.msg.__str__ (*self*)

Convert msg object to string.

Definition at line 442 of file xml_utils.py.

10.200.2.2 def rpki.xml_utils.msg.endElement (*self*, *stack*, *name*, *text*)

Handle top-level PDU.

Definition at line 434 of file xml_utils.py.

10.200.2.3 def rpki.xml_utils.msg.is_query (*self*)

Is this msg a query?

Definition at line 468 of file xml_utils.py.

10.200.2.4 def rpki.xml_utils.msg.is_reply (*self*)

Is this msg a reply?

Definition at line 472 of file xml_utils.py.

10.200.2.5 def rpki.xml_utils.msg.query (*cls*, *args*)

Create a query PDU.

Definition at line 455 of file xml_utils.py.

10.200.2.6 def rpki.xml_utils.msg.reply (*cls*, *args*)

Create a reply PDU.

Definition at line 462 of file xml_utils.py.

10.200.2.7 def rpki.xml_utils.msg.startElement (*self*, *stack*, *name*, *attrs*)

Handle top-level PDU.

Definition at line 421 of file xml_utils.py.

10.200.2.8 def rpki.xml_utils.msg.toXML (*self*)

Generate top-level PDU.

Definition at line 446 of file xml_utils.py.

10.200.3 Member Data Documentation**10.200.3.1 rpki.xml_utils.msg.type**

Definition at line 427 of file xml_utils.py.

10.200.3.2 rpki.xml_utils.msg.version

Reimplemented in [rpki.left_right.msg](#), and [rpki.publication.msg](#).

Definition at line 426 of file `xml_utils.py`.

The documentation for this class was generated from the following file:

- [xml_utils.py \(2791\)](#)

10.201 rpki.xml_utils.sax_handler Class Reference

Inherits [xml::sax::handler::ContentHandler](#).

Inherited by [rpki.left_right.sax_handler](#), [rpki.publication.sax_handler](#), and [rpki.up_down.sax_handler](#).

Public Member Functions

- def [__init__](#)
- def [characters](#)
- def [create_top_level](#)
- def [endElement](#)
- def [endElementNS](#)
- def [saxify](#)
- def [startElement](#)
- def [startElementNS](#)

Public Attributes

- [result](#)
- [stack](#)
- [text](#)

10.201.1 Detailed Description

SAX handler for RPKI protocols.

This class provides some basic amenities for parsing protocol XML of the kind we use in the RPKI protocols, including whacking all the protocol element text into US-ASCII, simplifying accumulation of text fields, and hiding some of the fun relating to XML namespaces.

General assumption: by the time this parsing code gets invoked, the

XML has already passed RelaxNG validation, so we only have to check for errors that the schema can't catch, and we don't have to play as many XML namespace games.

Definition at line 38 of file xml_utils.py.

10.201.2 Member Function Documentation

10.201.2.1 def rpki.xml_utils.sax_handler.__init__ (*self*)

Initialize SAX handler.

Definition at line 53 of file xml_utils.py.

10.201.2.2 def rpki.xml_utils.sax_handler.characters (*self*, *content*)

Accumulate a chunk of element content (text).

Definition at line 69 of file xml_utils.py.

10.201.2.3 def rpki.xml_utils.sax_handler.create_top_level (*self*, *name*, *attrs*)

Handle top-level PDU for this protocol.

Definition at line 119 of file xml_utils.py.

10.201.2.4 def rpki.xml_utils.sax_handler.endElement (*self*, *name*)

Handle endElement() events. Mostly this means handling any accumulated element text.

Definition at line 101 of file xml_utils.py.

10.201.2.5 def rpki.xml_utils.sax_handler.endElementNS (self, name, qname)

Redirect endElementNS() events to endElement().

Definition at line 65 of file xml_utils.py.

10.201.2.6 def rpki.xml_utils.sax_handler.saxify (cls, elt)

Create a one-off SAX parser, parse an ETree, return the result.

Definition at line 111 of file xml_utils.py.

10.201.2.7 def rpki.xml_utils.sax_handler.startElement (self, name, attrs)

Handle startElement() events.

We maintain a stack of nested elements under construction so that we can feed events directly to the current element rather than having to pass them through all the nesting elements.

If the stack is empty, this event is for the outermost element, so we call a virtual method to create the corresponding object and that's the object we'll be returning as our final result.

Definition at line 73 of file xml_utils.py.

10.201.2.8 def rpki.xml_utils.sax_handler.startElementNS (self, name, qname, attrs)

Redirect startElementNS() events to startElement().

Definition at line 61 of file xml_utils.py.

10.201.3 Member Data Documentation

10.201.3.1 rpki.xml_utils.sax_handler.result

Definition at line 97 of file xml_utils.py.

10.201.3.2 rpki.xml_utils.sax_handler.stack

Definition at line 59 of file xml_utils.py.

10.201.3.3 rpki.xml_utils.sax_handler.text

Definition at line 58 of file xml_utils.py.

The documentation for this class was generated from the following file:

- [xml_utils.py \(2791\)](#)

10.202 rpki.xml_utils.text_elt Class Reference

Inherits [rpki.xml_utils.base_elt](#).

Inherited by [rpki.left_right.list_published_objects_elt](#), [rpki.left_right.report_error_elt](#), and [rpki.publication.report_error_elt](#).

Public Member Functions

- def [endElement](#)
- def [toXML](#)

Static Public Attributes

- [text_attribute](#) = None
Name of the class attribute that holds the text value.

10.202.1 Detailed Description

Virtual base class for XML message elements that contain text.

Definition at line 219 of file xml_utils.py.

10.202.2 Member Function Documentation

10.202.2.1 def rpki.xml_utils.text_elt.endElement (self, stack, name, text)

Extract text from parsed XML.

Reimplemented from [rpki.xml_utils.base_elt](#).

Definition at line 228 of file xml_utils.py.

10.202.2.2 def rpki.xml_utils.text_elt.toXML (self)

Insert text into generated XML.

Reimplemented from [rpki.xml_utils.base_elt](#).

Definition at line 235 of file xml_utils.py.

10.202.3 Member Data Documentation

10.202.3.1 rpki::xml_utils.text_elt::text_attribute = None [static]

Name of the class attribute that holds the text value.

Reimplemented in [rpki.left_right.list_published_objects_elt](#), [rpki.left_right.report_error_elt](#), and [rpki.publication.report_error_elt](#).

Definition at line 226 of file xml_utils.py.

The documentation for this class was generated from the following file:

- [xml_utils.py \(2791\)](#)

10.203 Sequence Class Reference

Inherited by [rpki.manifest.FileAndHash](#), [rpki.manifest.Manifest](#), [rpki.roa.ROAIPAddress](#), [rpki.roa.ROAIPAddressFamily](#), and [rpki.roa.RouteOriginAttestation](#).

The documentation for this class was generated from the following file:

- [roa.py \(2424\)](#)

10.204 SequenceOf Class Reference

Inherited by [rpki.manifest.FilesAndHashes](#), [rpki.roa.ROAIPAddresses](#), and [rpki.roa.ROAIPAddressFamilies](#).

The documentation for this class was generated from the following file:

- [roa.py \(2424\)](#)

10.205 TextWrapper Class Reference

Inherited by [irbe_cli.UsageWrapper](#).

The documentation for this class was generated from the following file:

- [irbe_cli.py \(2799\)](#)

10.206 ContentHandler Class Reference

Inherited by [rpki.xml_utils.sax_handler](#).

The documentation for this class was generated from the following file:

- [xml_utils.py \(2791\)](#)

11 File Documentation

11.1 __init__.py File Reference

Packages

- package [rpki](#)

11.2 `async.py` File Reference

Classes

- 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.event_loop`
- def `rpki::async.exit_event_loop`

Variables

- `rpki::async.ExitNow` = `asyncore.ExitNow`

11.3 `config.py` File Reference

Classes

- class `rpki.config.parser`

Packages

- package `rpki.config`

11.4 `exceptions.py` File Reference

Classes

- class `rpki.exceptions.BadClassNameSyntax`
- class `rpki.exceptions.BadClientURL`
- class `rpki.exceptions.BadContactURL`
- class `rpki.exceptions.BadExtension`
- class `rpki.exceptions.BadIRDBReply`

- class [rpki.exceptions.BadIssueResponse](#)
- class [rpki.exceptions.BadPKCS10](#)
- class [rpki.exceptions.BadPublicationReply](#)
- class [rpki.exceptions.BadQuery](#)
- class [rpki.exceptions.BadSender](#)
- class [rpki.exceptions.BadStatusCode](#)
- class [rpki.exceptions.BadURISyntax](#)
- class [rpki.exceptions.BSCNotFound](#)
- class [rpki.exceptions.BSCNotReady](#)
- class [rpki.exceptions.ChildNotFound](#)
- class [rpki.exceptions.ClassNameMismatch](#)
- class [rpki.exceptions.ClassNameUnknown](#)
- class [rpki.exceptions.ClientNotFound](#)
- class [rpki.exceptions.CMSCRLNotSet](#)
- class [rpki.exceptions.CMSVerificationFailed](#)
- class [rpki.exceptions.DBConsistencyError](#)
- class [rpki.exceptions.DERObjectConversionError](#)
- class [rpki.exceptions.DuplicateObject](#)
- class [rpki.exceptions.EmptyPEM](#)
- class [rpki.exceptions.EmptyROAPrefixList](#)
- class [rpki.exceptions.ForbiddenURI](#)
- class [rpki.exceptions.HandleTranslationError](#)
- class [rpki.exceptions.HTTPRequestFailed](#)
- class [rpki.exceptions.HTTPSBadVersion](#)
- class [rpki.exceptions.HTTPSClientAborted](#)
- class [rpki.exceptions.HTTPSUnexpectedState](#)
- class [rpki.exceptions.MissingCMSCRL](#)
- class [rpki.exceptions.MissingCMSEECert](#)
- class [rpki.exceptions.MultipleTLSEECert](#)
- class [rpki.exceptions.MustBePrefix](#)
- class [rpki.exceptions.NoActiveCA](#)
- class [rpki.exceptions.NoCoveringCertForROA](#)
- class [rpki.exceptions.NoObjectAtURI](#)
- class [rpki.exceptions.NotACertificateChain](#)
- class [rpki.exceptions.NotFound](#)
- class [rpki.exceptions.NotImplementedYet](#)
- class [rpki.exceptions.NotInDatabase](#)
- class [rpki.exceptions.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](#)

11.5 https.py File Reference

Classes

- class [rpki.https.http_client](#)
- class [rpki.https.http_listener](#)
- class [rpki.https.http_message](#)
- class [rpki.https.http_queue](#)
- class [rpki.https.http_request](#)
- class [rpki.https.http_response](#)
- class [rpki.https.http_server](#)
- class [rpki.https.http_stream](#)

Packages

- package [rpki.https](#)

Functions

- def [rpki::https.build_https_ta_cache](#)
- def [rpki::https.client](#)
- def [rpki::https.logger](#)
- def [rpki::https.server](#)

Variables

- dictionary [rpki::https.client_queues](#) = { }
- [rpki::https.debug_http](#) = False
- [rpki::https.debug_tls_certs](#) = False
- tuple [rpki::https.default_client_timeout](#) = [rpki.sundial.timedelta](#)(minutes = 15)
- tuple [rpki::https.default_http_version](#) = (1, 0)

- tuple `rpki::https.default_server_timeout` = `rpki.sundial.timedelta(minutes = 20)`
- string `rpki::https.rpki_content_type` = "application/x-rpki"
- `rpki::https.want_persistent_client` = True
- `rpki::https.want_persistent_server` = True

11.6 ipaddrs.py File Reference

Classes

- class `rpki.ipaddrs.v4addr`
- class `rpki.ipaddrs.v6addr`

Packages

- package `rpki.ipaddrs`

11.7 irbe_cli.py File Reference

Classes

- class `irbe_cli.bsc_elt`
- class `irbe_cli.caller`
- 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_sax_handler`
- class `irbe_cli.list_published_objects_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_sax_handler`
- class `irbe_cli.reply_elt_mixin`
- class `irbe_cli.report_error_elt`
- class `irbe_cli.report_error_elt`
- class `irbe_cli.repository_elt`

- class [irbe_cli.roa_elt](#)
- class [irbe_cli.self_elt](#)
- class [irbe_cli.UsageWrapper](#)

Packages

- package [irbe_cli](#)

Functions

- def [irbe_cli.usage](#)

Variables

- list [irbe_cli.argv](#) = sys.argv[1:]
- tuple [irbe_cli.call_pubd](#)
- tuple [irbe_cli.call_rpkid](#)
- tuple [irbe_cli.cfg](#) = [rpki.config.parser](#)(cfg_file, "irbe_cli")
- string [irbe_cli.cfg_file](#) = "irbe.conf"
- [irbe_cli.pem_out](#) = None
- [irbe_cli.q_msg](#) = q_msg_left_right
- tuple [irbe_cli.q_msg_left_right](#) = left_right_msg.query()
- tuple [irbe_cli.q_msg_publication](#) = publication_msg.query()
- list [irbe_cli.q_pdu](#) = left_right_msg.pdus[argv[0]]
- list [irbe_cli.top_opts](#) = ["config=", "help", "pem_out=", "quiet", "verbose"]
- tuple [irbe_cli.usage_fill](#) = UsageWrapper(subsequent_indent = " " * 4)
- [irbe_cli.verbose](#) = True

11.8 irdbd.py File Reference

Packages

- package [irdbd](#)

Functions

- def [irdbd.handle_list_resources](#)
- def [irdbd.handle_list_roa_requests](#)
- def [irdbd.handler](#)

Variables

- tuple `irdbd.bpki_ta` = `rpki.x509.X509`(Auto_file = `cfg.get("bpki-ta")`)
- tuple `irdbd.cfg` = `rpki.config.parser`(`cfg_file`, "irdbd")
- string `irdbd.cfg_file` = "irdbd.conf"
- tuple `irdbd.client_ta` = (`bpki_ta`, `rpkiid_cert`)
- tuple `irdbd.cur` = `db.cursor()`
- tuple `irdbd.db`
- dictionary `irdbd.handle_dispatch`
- tuple `irdbd.handlers` = ((`u.path`, `handler`),)
- string `irdbd.host` = "localhost"
- tuple `irdbd.irdbd_cert` = `rpki.x509.X509`(Auto_file = `cfg.get("irdbd-cert")`)
- tuple `irdbd.irdbd_key` = `rpki.x509.RSA`(Auto_file = `cfg.get("irdbd-key")`)
- int `irdbd.port` = 443
- tuple `irdbd.rpkiid_cert` = `rpki.x509.X509`(Auto_file = `cfg.get("rpkiid-cert")`)
- `irdbd.server_cert` = `irdbd_cert`,
- tuple `irdbd.startup_msg` = `cfg.get("startup-message", "")`
- tuple `irdbd.u` = `urlparse.urlparse`(`cfg.get("https-url")`)

11.9 left_right.py File Reference

Classes

- class `rpki.left_right.bsc_elt`
- class `rpki.left_right.child_elt`
- class `rpki.left_right.cms_msg`
- class `rpki.left_right.data_elt`
- class `rpki.left_right.left_right_namespace`
- class `rpki.left_right.list_published_objects_elt`
- class `rpki.left_right.list_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

11.10 log.py File Reference

Classes

- class `rpki.log.logger`

Packages

- package `rpki.log`

Functions

- def `rpki::log.init`
- def `rpki::log.set_trace`
- def `rpki::log.trace`
- def `rpki::log.traceback`

Variables

- tuple `rpki::log.debug` = `logger(syslog.LOG_DEBUG)`
- `rpki::log.enable_trace` = False
Whether call tracing is enabled.
- tuple `rpki::log.error` = `logger(syslog.LOG_ERR)`
- tuple `rpki::log.info` = `logger(syslog.LOG_INFO)`
- tuple `rpki::log.note` = `logger(syslog.LOG_NOTICE)`
- int `rpki::log.pid` = 0
- string `rpki::log.tag` = ""
- `rpki::log.use_syslog` = False
Whether to use syslog.
- tuple `rpki::log.warn` = `logger(syslog.LOG_WARNING)`

11.11 manifest.py File Reference

Classes

- class [rpki.manifest.FileAndHash](#)
- class [rpki.manifest.FilesAndHashes](#)
- class [rpki.manifest.Manifest](#)

Packages

- package [rpki.manifest](#)

11.12 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.

11.13 pubd.py File Reference

Classes

- class [pubd.pubd_context](#)

Packages

- package [pubd](#)

Functions

- def [pubd.main](#)

Variables

- string `pubd.cfg_file` = "pubd.conf"
- `pubd.profile` = False

11.14 publication.py File Reference

Classes

- class `rpki.publication.certificate_elt`
- class `rpki.publication.client_elt`
- class `rpki.publication.cms_msg`
- class `rpki.publication.config_elt`
- class `rpki.publication.control_elt`
- class `rpki.publication.crl_elt`
- class `rpki.publication.manifest_elt`
- class `rpki.publication.msg`
- class `rpki.publication.publication_namespace`
- class `rpki.publication.publication_object_elt`
- class `rpki.publication.report_error_elt`
- class `rpki.publication.roa_elt`
- class `rpki.publication.sax_handler`

Packages

- package `rpki.publication`

11.15 relaxng.py File Reference

Packages

- package `rpki.relaxng`

Variables

- tuple `rpki::relaxng.left_right`
Parsed RelaxNG `left_right` schema.
- tuple `rpki::relaxng.publication`
Parsed RelaxNG `publication` schema.
- tuple `rpki::relaxng.up_down`

Parsed RelaxNG [up_down](#) schema.

11.16 resource_set.py File Reference

Classes

- class [rpki.resource_set.resource_bag](#)
- class [rpki.resource_set.resource_range](#)
- class [rpki.resource_set.resource_range_as](#)
- class [rpki.resource_set.resource_range_ip](#)
- class [rpki.resource_set.resource_range_ipv4](#)
- class [rpki.resource_set.resource_range_ipv6](#)
- class [rpki.resource_set.resource_set](#)
- class [rpki.resource_set.resource_set_as](#)
- class [rpki.resource_set.resource_set_ip](#)
- class [rpki.resource_set.resource_set_ipv4](#)
- class [rpki.resource_set.resource_set_ipv6](#)
- class [rpki.resource_set.roa_prefix](#)
- class [rpki.resource_set.roa_prefix_ipv4](#)
- class [rpki.resource_set.roa_prefix_ipv6](#)
- class [rpki.resource_set.roa_prefix_set](#)
- class [rpki.resource_set.roa_prefix_set_ipv4](#)
- class [rpki.resource_set.roa_prefix_set_ipv6](#)

Packages

- package [rpki.resource_set](#)

Functions

- def [rpki::resource_set._bs2long](#)
- def [rpki::resource_set._long2bs](#)
- def [rpki::resource_set._rsplit](#)
- def [rpki::resource_set.test1](#)
- def [rpki::resource_set.test2](#)

Variables

- string [rpki::resource_set.inherit_token](#) = "<inherit>"
Token used to indicate inheritance in read and print syntax.

11.17 roa.py File Reference

Classes

- class [rpki.roa.ROAIPAddress](#)
- class [rpki.roa.ROAIPAddresses](#)
- class [rpki.roa.ROAIPAddressFamilies](#)
- class [rpki.roa.ROAIPAddressFamily](#)
- class [rpki.roa.RouteOriginAttestation](#)

Packages

- package [rpki.roa](#)

11.18 rootd.py File Reference

Classes

- class [rootd.cms_msg](#)
- class [rootd.issue_pdu](#)
- class [rootd.list_pdu](#)
- class [rootd.message_pdu](#)
- class [rootd.revoke_pdu](#)
- class [rootd.sax_handler](#)

Packages

- package [rootd](#)

Functions

- def [rootd.compose_response](#)
- def [rootd.del_subject_cert](#)
- def [rootd.del_subject_pkcs10](#)
- def [rootd.get_root_cert](#)
- def [rootd.get_subject_cert](#)
- def [rootd.get_subject_pkcs10](#)
- def [rootd.issue_subject_cert_maybe](#)
- def [rootd.root_newer_than_subject](#)
- def [rootd.set_subject_cert](#)
- def [rootd.set_subject_pkcs10](#)
- def [rootd.up_down_handler](#)

Variables

- tuple `rootd.bpki_ta` = `rpki.x509.X509`(`Auto_file` = `cfg.get("bpki-ta")`)
- tuple `rootd.cfg` = `rpki.config.parser`(`cfg_file`, "rootd")
- string `rootd.cfg_file` = "rootd.conf"
- tuple `rootd.child_bpki_cert` = `rpki.x509.X509`(`Auto_file` = `cfg.get("child-bpki-cert")`)
- tuple `rootd.client_ta` = (`bpki_ta`, `child_bpki_cert`)
- `rootd.handlers` = `up_down_handler`)
- `rootd.host` = `https_server_host`,
- tuple `rootd.https_server_host` = `cfg.get("server-host", "")`
- tuple `rootd.https_server_port` = `int(cfg.get("server-port"))`
- `rootd.port` = `https_server_port`,
- tuple `rootd.rootd_bpki_cert` = `rpki.x509.X509`(`Auto_file` = `cfg.get("rootd-bpki-cert")`)
- tuple `rootd.rootd_bpki_crl` = `rpki.x509.CRL`(`Auto_file` = `cfg.get("rootd-bpki-crl")`)
- tuple `rootd.rootd_bpki_key` = `rpki.x509.RSA`(`Auto_file` = `cfg.get("rootd-bpki-key")`)
- tuple `rootd.rpki_base_uri` = `cfg.get("rpki-base-uri", "rsync://" + rpki_class_name + ".invalid/")`
- tuple `rootd.rpki_class_name` = `cfg.get("rpki-class-name", "wombat")`
- `rootd.rpki_root_cert` = `None`
- tuple `rootd.rpki_root_cert_file` = `cfg.get("rpki-root-cert")`
- tuple `rootd.rpki_root_cert_uri` = `cfg.get("rpki-root-cert-uri", rpki_base_uri + "Root.cer")`
- tuple `rootd.rpki_root_crl` = `cfg.get("rpki-root-crl", "Root.crl")`
- tuple `rootd.rpki_root_dir` = `cfg.get("rpki-root-dir")`
- tuple `rootd.rpki_root_key` = `rpki.x509.RSA`(`Auto_file` = `cfg.get("rpki-root-key")`)
- tuple `rootd.rpki_root_manifest` = `cfg.get("rpki-root-manifest", "Root.mnf")`
- tuple `rootd.rpki_subject_cert` = `cfg.get("rpki-subject-cert", "Child.cer")`
- tuple `rootd.rpki_subject_lifetime` = `rpki.sundial.timedelta.parse(cfg.get("rpki-subject-lifetime", "30d"))`
- tuple `rootd.rpki_subject_pkcs10` = `cfg.get("rpki-subject-pkcs10", "Child.pkcs10")`
- tuple `rootd.rpki_subject_regen` = `rpki.sundial.timedelta.parse(cfg.get("rpki-subject-regen", rpki_subject_lifetime.convert_to_seconds() / 2))`
- `rootd.server_cert` = `rootd_bpki_cert`,

11.19 rpki_engine.py File Reference

Classes

- class [rpki.rpki_engine.ca_detail_obj](#)
- class [rpki.rpki_engine.ca_obj](#)
- class [rpki.rpki_engine.child_cert_obj](#)
- class [rpki.rpki_engine.revoked_cert_obj](#)
- class [rpki.rpki_engine.roa_obj](#)
- class [rpki.rpki_engine.rpkid_context](#)

Packages

- package [rpki.rpki_engine](#)

11.20 rpkid.py File Reference

Packages

- package [rpkid](#)

Functions

- def [rpkid.main](#)

Variables

- string [rpkid.cfg_file](#) = "rpkid.conf"
- [rpkid.profile](#) = None

11.21 sql.py File Reference

Classes

- class [rpki.sql.session](#)
- class [rpki.sql.sql_persistent](#)
- class [rpki.sql.template](#)

Packages

- package [rpki.sql](#)

11.22 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](#)

11.23 up_down.py File Reference

Classes

- class [rpki.up_down.base_elt](#)
- class [rpki.up_down.certificate_elt](#)
- class [rpki.up_down.class_elt](#)
- class [rpki.up_down.class_response_syntax](#)
- class [rpki.up_down.cms_msg](#)
- class [rpki.up_down.error_response_pdu](#)
- class [rpki.up_down.issue_pdu](#)
- class [rpki.up_down.issue_response_pdu](#)
- class [rpki.up_down.list_pdu](#)
- class [rpki.up_down.list_response_pdu](#)
- class [rpki.up_down.message_pdu](#)
- class [rpki.up_down.multi_uri](#)
- class [rpki.up_down.revoke_pdu](#)
- class [rpki.up_down.revoke_response_pdu](#)
- class [rpki.up_down.revoke_syntax](#)
- class [rpki.up_down.sax_handler](#)

Packages

- package [rpki.up_down](#)

Variables

- dictionary `rpki::up_down.nsmap` = { None : xmlns }
- string `rpki::up_down.xmlns` = "http://www.apnic.net/specs/rescerts/up-down/"

11.24 x509.py File Reference

Classes

- class `rpki.x509.CMS_object`
- class `rpki.x509.CRL`
- class `rpki.x509.DER_CMS_object`
- class `rpki.x509.DER_object`
- class `rpki.x509.PEM_converter`
- class `rpki.x509.PKCS10`
- class `rpki.x509.ROA`
- class `rpki.x509.RSA`
- class `rpki.x509.RSAPublic`
- class `rpki.x509.SignedManifest`
- class `rpki.x509.X509`
- class `rpki.x509.XML_CMS_object`

Packages

- package `rpki.x509`

Functions

- def `rpki::x509.calculate_SKI`
- def `rpki::x509.POWify_OID`

11.25 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`, 325
 - `__add__`
 - `rpki::sundial::datetime`, 321
 - `rpki::sundial::timedelta`, 325
 - `__call__`
 - `irbe_cli::caller`, 97
 - `irbe_cli::UsageWrapper`, 113
 - `rpki::async::iterator`, 123
 - `rpki::async::sync_wrapper`, 126
 - `rpki::log::logger`, 220
 - `__cmp__`
 - `rpki::async::timer`, 128
 - `rpki::resource_set::resource_range`, 249
 - `rpki::resource_set::roa_prefix`, 264
 - `rpki::x509::DER_object`, 366
 - `__div__`
 - `rpki::sundial::timedelta`, 325
 - `__eq__`
 - `rpki::resource_set::resource_bag`, 246
 - `__floordiv__`
 - `rpki::sundial::timedelta`, 326
 - `__init__`
 - `irbe_cli::caller`, 97
 - `pubd::pubd_context`, 115
 - `rpki::async::iterator`, 123
 - `rpki::async::sync_wrapper`, 126
 - `rpki::async::timer`, 128
 - `rpki::config::parser`, 132
 - `rpki::https::http_client`, 153
 - `rpki::https::http_listener`, 157
 - `rpki::https::http_message`, 160
 - `rpki::https::http_queue`, 162
 - `rpki::https::http_request`, 165
 - `rpki::https::http_response`, 166
 - `rpki::https::http_server`, 168
 - `rpki::https::http_stream`, 172
 - `rpki::log::logger`, 220
 - `rpki::manifest::FileAndHash`, 221
 - `rpki::manifest::FilesAndHashes`, 222
 - `rpki::manifest::Manifest`, 222
 - `rpki::resource_set::resource_bag`, 246
 - `rpki::resource_set::resource_range`, 249
 - `rpki::resource_set::resource_set`, 255
 - `rpki::resource_set::roa_prefix`, 264
 - `rpki::resource_set::roa_prefix_set`, 268
 - `rpki::roa::ROAIPAddress`, 272
 - `rpki::roa::ROAIPAddresses`, 273
 - `rpki::roa::ROAIPAddressFamilies`, 274
 - `rpki::roa::ROAIPAddressFamily`, 274
 - `rpki::roa::RouteOriginAttestation`, 275
 - `rpki::rpki_engine::child_cert_obj`, 291
 - `rpki::rpki_engine::revoked_cert_obj`, 295
 - `rpki::rpki_engine::roa_obj`, 297
 - `rpki::rpki_engine::rpkid_context`, 303
 - `rpki::sql::session`, 309
 - `rpki::sql::template`, 318
 - `rpki::up_down::class_elt`, 333
 - `rpki::up_down::class_response_syntax`, 336
 - `rpki::up_down::error_response_pdu`, 339
 - `rpki::up_down::multi_uri`, 350
 - `rpki::x509::DER_object`, 366
 - `rpki::x509::PEM_converter`, 373
 - `rpki::xml_utils::sax_handler`, 405
 - `__init__.py(2589)`, 409
 - `__mul__`
 - `rpki::sundial::timedelta`, 326
 - `__ne__`
 - `rpki::resource_set::resource_bag`, 246
 - `__neg__`

- rpki::sundial::timedelta, 326
- __new__
 - rpki::ipaddr::v4addr, 177
 - rpki::ipaddr::v6addr, 178
- __pos__
 - rpki::sundial::timedelta, 326
- __radd__
 - rpki::sundial::datetime, 321
 - rpki::sundial::timedelta, 326
- __rdiv__
 - rpki::sundial::timedelta, 326
- __repr__
 - rpki::async::iterator, 124
 - rpki::async::timer, 128
- __rfloordiv__
 - rpki::sundial::timedelta, 326
- __rmul__
 - rpki::sundial::timedelta, 327
- __rsub__
 - rpki::sundial::datetime, 321
 - rpki::sundial::timedelta, 327
- __str__
 - rpki::https::http_message, 160
 - rpki::ipaddr::v4addr, 177
 - rpki::ipaddr::v6addr, 178
 - rpki::publication::report_error_elt, 241
 - rpki::resource_set::resource_bag, 246
 - rpki::resource_set::resource_range_as, 250
 - rpki::resource_set::resource_range_ip, 252
 - rpki::resource_set::resource_set, 255
 - rpki::resource_set::roa_prefix, 264
 - rpki::resource_set::roa_prefix_set, 268
 - rpki::sundial::datetime, 321
 - rpki::up_down::message_pdu, 347
 - rpki::up_down::multi_uri, 350
 - rpki::xml_utils::base_elt, 394
 - rpki::xml_utils::msg, 402
- __sub__
 - rpki::sundial::datetime, 321
 - rpki::sundial::timedelta, 327
- __bs2long
 - rpki::resource_set, 83
- _cast
 - rpki::sundial, 88
- _comm
 - rpki::resource_set::resource_set, 255
- _exceptions_enabled
 - rpki::sql::session, 311
- _get_wrapper
 - rpki::config::parser, 132
- _long2bs
 - rpki::resource_set, 83
- _prefixlen
 - rpki::resource_set::resource_range_ip, 252
- _raiseExitNow
 - rpki::async, 64
- _rsplit
 - rpki::resource_set, 83
- _wrap_execute
 - rpki::sql::session, 309
- activate
 - rpki::rpki_engine::ca_detail_obj, 278
- address
 - rpki::roa::ROAIPAddress, 272
- addresses
 - rpki::roa::ROAIPAddressFamily, 275
- addressFamily
 - rpki::roa::ROAIPAddressFamily, 275
- afi
 - rpki::resource_set::resource_set_ipv4, 262
 - rpki::resource_set::resource_set_ipv6, 263
- argv
 - irbe_cli, 47
- asID
 - rpki::roa::RouteOriginAttestation, 276
- asn
 - rpki::left_right::list_resources_elt, 196

- rpki::resource_set::resource_bag, 247
- rpki::rpki_engine::roa_obj, 300
- assert_pristine
 - rpki::sql::session, 309
- async.py(2748), 410
- asynchat::async_chat, 94
- asyncore::dispatcher, 95
- attributes
 - rpki::left_right::bsc_elt, 181
 - rpki::left_right::child_elt, 186
 - rpki::left_right::list_published_objects_elt, 194
 - rpki::left_right::list_resources_elt, 196
 - rpki::left_right::list_roa_requests_elt, 198
 - rpki::left_right::parent_elt, 203
 - rpki::left_right::report_error_elt, 206
 - rpki::left_right::repository_elt, 209
 - rpki::left_right::self_elt, 217
 - rpki::publication::client_elt, 227
 - rpki::publication::config_elt, 231
 - rpki::publication::publication_object_elt, 240
 - rpki::publication::report_error_elt, 242
 - rpki::xml_utils::base_elt, 396
- b
 - rpki::x509::PEM_converter, 373
- base_uri
 - rpki::publication::client_elt, 227
- bits
 - rpki::ipaddrs::v4addr, 177
 - rpki::ipaddrs::v6addr, 179
- body
 - rpki::https::http_message, 161
- booleans
 - rpki::left_right::bsc_elt, 181
 - rpki::left_right::child_elt, 186
 - rpki::left_right::parent_elt, 203
 - rpki::left_right::self_elt, 217
 - rpki::xml_utils::base_elt, 396
- bpki_cert
 - irbe_cli::cmd_elt_mixin, 102
- rpki::left_right::child_elt, 186
- rpki::left_right::repository_elt, 209
- rpki::left_right::self_elt, 218
- rpki::publication::client_elt, 227
- bpki_cms_cert
 - irbe_cli::cmd_elt_mixin, 102
 - rpki::left_right::parent_elt, 203
- bpki_cms_glue
 - irbe_cli::cmd_elt_mixin, 102
 - rpki::left_right::parent_elt, 204
- bpki_crl
 - irbe_cli::config_elt, 105
- bpki_glue
 - irbe_cli::cmd_elt_mixin, 102
 - rpki::left_right::child_elt, 186
 - rpki::left_right::repository_elt, 209
 - rpki::left_right::self_elt, 218
 - rpki::publication::client_elt, 227
- bpki_https_cert
 - irbe_cli::cmd_elt_mixin, 103
 - rpki::left_right::parent_elt, 204
- bpki_https_glue
 - irbe_cli::cmd_elt_mixin, 103
 - rpki::left_right::parent_elt, 204
- bpki_ta
 - irdbd, 51
 - pubd::pubd_context, 116
 - rootd, 59
 - rpki::rpki_engine::rpkid_context, 305
- bsc
 - rpki::left_right::data_elt, 189
- bscs
 - rpki::left_right::self_elt, 213
- buffer
 - rpki::https::http_stream, 175
- build
 - rpki::x509::ROA, 377
 - rpki::x509::SignedManifest, 384
- build_https_ta_cache
 - pubd::pubd_context, 115
 - rpki::https, 69
 - rpki::rpki_engine::rpkid_context, 303
- ca

- rpki::rpki_engine::ca_detail_obj, 278
- ca_cert_uri
 - rpki::rpki_engine::ca_detail_obj, 282
- ca_detail
 - rpki::rpki_engine::child_cert_obj, 291
 - rpki::rpki_engine::revoked_cert_obj, 295
 - rpki::rpki_engine::roa_obj, 297
- ca_detail_id
 - rpki::rpki_engine::child_cert_obj, 293
 - rpki::rpki_engine::revoked_cert_obj, 295
 - rpki::rpki_engine::roa_obj, 300
- ca_details
 - rpki::rpki_engine::ca_obj, 285
- ca_from_class_name
 - rpki::left_right::child_elt, 184
- ca_id
 - rpki::rpki_engine::ca_detail_obj, 282
- cache
 - rpki::sql::session, 311
- cache_clear
 - rpki::sql::session, 309
- calculate_SKI
 - rpki::x509, 92
- call_pubd
 - irbe_cli, 47
 - rpki::left_right::repository_elt, 208
- call_rpkid
 - irbe_cli, 47
- callback
 - rpki::https::http_request, 165
- caller_function
 - rpki::async::iterator, 124
- cancel
 - rpki::async::timer, 128
- cas
 - rpki::left_right::parent_elt, 201
- cb
 - rpki::async::sync_wrapper, 126
- cert
 - rpki::https::http_client, 155
 - rpki::https::http_listener, 158
 - rpki::https::http_queue, 163
 - rpki::rpki_engine::child_cert_obj, 293
 - rpki::rpki_engine::roa_obj, 300
 - rpki::up_down::certificate_elt, 332
- cert_url
 - rpki::up_down::certificate_elt, 332
 - rpki::up_down::class_elt, 335
- certs
 - rpki::up_down::class_elt, 335
- cfg
 - irbe_cli, 47
 - irdbd, 51
 - rootd, 59
 - rpki::config::parser, 134
- cfg_file
 - irbe_cli, 47
 - irdbd, 51
 - pubd, 55
 - rootd, 59
 - rpkid, 94
- characters
 - rpki::xml_utils::sax_handler, 405
- check_allowed_uri
 - rpki::publication::client_elt, 225
- check_for_updates
 - rpki::rpki_engine::ca_obj, 285
- check_response
 - rpki::up_down::base_elt, 329
 - rpki::up_down::error_response_pdu, 339
 - rpki::up_down::issue_response_pdu, 344
- check_valid_rpkid
 - rpki::x509::PKCS10, 375
- child
 - rpki::rpki_engine::child_cert_obj, 291
- child_bpki_cert
 - rootd, 59
- child_certs
 - rpki::left_right::child_elt, 184
 - rpki::rpki_engine::ca_detail_obj, 278

- child_id
 - rpki::rpki_engine::child_cert_obj, 293
- children
 - rpki::left_right::bsc_elt, 180
 - rpki::left_right::self_elt, 213
- chunk_body
 - rpki::https::http_stream, 172
- chunk_discard_crlf
 - rpki::https::http_stream, 172
- chunk_discard_trailer
 - rpki::https::http_stream, 172
- chunk_handler
 - rpki::https::http_stream, 175
- chunk_header
 - rpki::https::http_stream, 172
- class_name
 - rpki::up_down::class_elt, 335
 - rpki::up_down::issue_pdu, 343
 - rpki::up_down::revoke_pdu, 352
 - rpki::up_down::revoke_syntax, 354
- classes
 - rpki::up_down::class_response_syntax, 337
- clear
 - rpki::async::timer, 128
 - rpki::x509::DER_object, 367
- clear_https_ta_cache
 - pubd::pubd_context, 115
 - rpki::left_right::child_elt, 187
 - rpki::publication::client_elt, 227
 - rpki::rpki_engine::rpkid_context, 303
- client
 - rpki::https, 69
 - rpki::https::http_queue, 163
- client_cert
 - irbe_cli::caller, 98
- client_getopt
 - irbe_cli::cmd_elt_mixin, 101
- client_handler
 - pubd::pubd_context, 115
- client_key
 - irbe_cli::caller, 98
- client_poll
 - rpki::left_right::self_elt, 213
- client_query_bpki_cert
 - irbe_cli::cmd_elt_mixin, 101
- client_query_bpki_cms_cert
 - irbe_cli::cmd_elt_mixin, 101
- client_query_bpki_crl
 - irbe_cli::config_elt, 105
- client_query_bpki_https_cert
 - irbe_cli::cmd_elt_mixin, 101
- client_query_cms_glue
 - irbe_cli::cmd_elt_mixin, 101
- client_query_glue
 - irbe_cli::cmd_elt_mixin, 101
- client_query_https_glue
 - irbe_cli::cmd_elt_mixin, 102
- client_query_signing_cert
 - irbe_cli::bsc_elt, 96
- client_query_signing_cert_crl
 - irbe_cli::bsc_elt, 96
- client_queues
 - rpki::https, 70
- client_reply_decode
 - irbe_cli::bsc_elt, 96
 - irbe_cli::reply_elt_mixin, 111
- client_reply_show
 - irbe_cli::reply_elt_mixin, 111
- client_ta
 - irdbd, 51
 - rootd, 59
- client_url_regexp
 - pubd::pubd_context, 116
- close
 - rpki::https::http_stream, 172
 - rpki::sql::session, 309
- cmd
 - rpki::https::http_request, 165
- cms_class
 - irbe_cli::caller, 98
- code
 - rpki::https::http_response, 167
- codes
 - rpki::up_down::error_response_pdu, 340
- collect_incoming_data
 - rpki::https::http_stream, 172
- columns
 - rpki::sql::template, 318

- compose_response
 - rootd, 57
- config.py(2637), 410
- config_id
 - rpki::publication::config_elt, 231
- connect
 - rpki::sql::session, 309
- construct_sia_uri
 - rpki::rpki_engine::ca_obj, 286
- contains
 - rpki::resource_set::resource_set, 256
- content
 - rpki::x509::CMS_object, 358
 - rpki::x509::DER_CMS_object, 365
 - rpki::x509::XML_CMS_object, 393
- content_class
 - rpki::x509::ROA, 378
 - rpki::x509::SignedManifest, 385
- control_handler
 - pubd::pubd_context, 116
- convert_to_seconds
 - rpki::sundial::timedelta, 327
- create
 - rpki::rpki_engine::ca_detail_obj, 278
 - rpki::rpki_engine::ca_obj, 286
 - rpki::x509::PKCS10, 375
- create_ca
 - rpki::x509::PKCS10, 375
- create_top_level
 - rpki::xml_utils::sax_handler, 405
- crl_interval
 - rpki::left_right::self_elt, 218
- crl_uri
 - rpki::rpki_engine::ca_detail_obj, 278
- crl_uri_tail
 - rpki::rpki_engine::ca_detail_obj, 278
- cron
 - rpki::left_right::self_elt, 213
 - rpki::rpki_engine::rpkid_context, 303
- cron_keepalive
 - rpki::rpki_engine::rpkid_context, 305
- cron_period
 - rpki::rpki_engine::rpkid_context, 305
- cron_timeout
 - rpki::rpki_engine::rpkid_context, 305
- cronjob_handler
 - rpki::rpki_engine::rpkid_context, 304
- cross_certify
 - rpki::x509::X509, 387
- cur
 - irdbd, 51
 - rpki::sql::session, 311
- database
 - rpki::sql::session, 311
- datum_type
 - rpki::resource_set::resource_range_as, 251
 - rpki::resource_set::resource_range_ipv4, 253
 - rpki::resource_set::resource_range_ipv6, 254
- db
 - irdbd, 51
 - rpki::sql::session, 311
- debug
 - rpki::log, 76
- debug_cms_certs
 - rpki::x509::CMS_object, 358
- debug_http
 - rpki::https, 70
- debug_tls_certs
 - rpki::https, 70
- decode
 - rpki::x509::DER_CMS_object, 364
 - rpki::x509::XML_CMS_object, 391
- default_client_timeout
 - rpki::https, 70
- default_http_version
 - rpki::https, 70
- default_section
 - rpki::config::parser, 134
- default_server_timeout
 - rpki::https, 71

- del_subject_cert
 - rootd, 57
- del_subject_pkcs10
 - rootd, 57
- delete
 - rpki::rpki_engine::ca_detail_obj, 279
 - rpki::rpki_engine::ca_obj, 286
 - rpki::sql::template, 318
- DER
 - rpki::x509::CMS_object, 358
 - rpki::x509::CRL, 363
 - rpki::x509::DER_object, 371
 - rpki::x509::PKCS10, 376
 - rpki::x509::RSA, 380
 - rpki::x509::RSAPublic, 383
 - rpki::x509::X509, 389
- description
 - rpki::up_down::error_response_pdu, 340
- detach
 - rpki::https::http_queue, 162
- difference
 - rpki::resource_set::resource_set, 256
- dirty
 - rpki::sql::session, 311
- doit
 - rpki::async::iterator, 124
- done_callback
 - rpki::async::iterator, 124
- dump_inbound_cms
 - rpki::x509::XML_CMS_object, 393
- dump_on_verify_failure
 - rpki::x509::CMS_object, 359
- dump_outbound_cms
 - rpki::x509::XML_CMS_object, 393
- dump_to_disk
 - rpki::x509::XML_CMS_object, 391
- dumpasn1
 - rpki::x509::DER_object, 367
- dynamic_ta
 - rpki::https::http_listener, 158
- e
 - rpki::x509::PEM_converter, 373
- earlier
 - rpki::sundial::datetime, 321
- eb
 - rpki::async::sync_wrapper, 126
- econtent_oid
 - rpki::x509::CMS_object, 359
 - rpki::x509::ROA, 378
 - rpki::x509::SignedManifest, 385
 - rpki::x509::XML_CMS_object, 393
- element_name
 - rpki::left_right::bsc_elt, 182
 - rpki::left_right::child_elt, 187
 - rpki::left_right::list_published_objects_elt, 194
 - rpki::left_right::list_resources_elt, 196
 - rpki::left_right::list_roa_requests_elt, 198
 - rpki::left_right::parent_elt, 204
 - rpki::left_right::report_error_elt, 206
 - rpki::left_right::repository_elt, 210
 - rpki::left_right::self_elt, 218
 - rpki::publication::certificate_elt, 224
 - rpki::publication::client_elt, 227
 - rpki::publication::config_elt, 231
 - rpki::publication::crl_elt, 233
 - rpki::publication::manifest_elt, 234
 - rpki::publication::report_error_elt, 242
 - rpki::publication::roa_elt, 243
- elements
 - rpki::left_right::bsc_elt, 182
 - rpki::left_right::child_elt, 187
 - rpki::left_right::parent_elt, 204
 - rpki::left_right::repository_elt, 210
 - rpki::left_right::self_elt, 218
 - rpki::publication::client_elt, 227
 - rpki::publication::config_elt, 231
 - rpki::xml_utils::base_elt, 397
- empty
 - rpki::resource_set::resource_bag, 246
 - rpki::x509::DER_object, 367
- enable_trace
 - rpki::log, 76
- encode
 - rpki::x509::DER_CMS_object, 364

- rpki::x509::XML_CMS_object, 391
- encoding
 - rpki::left_right::cms_msg, 188
 - rpki::publication::cms_msg, 229
 - rpki::up_down::cms_msg, 338
- endElement
 - rpki::left_right::child_elt, 185
 - rpki::publication::client_elt, 225
 - rpki::publication::publication_ - object_elt, 238
 - rpki::up_down::base_elt, 329
 - rpki::up_down::certificate_elt, 331
 - rpki::up_down::class_elt, 333
 - rpki::up_down::error_response_pdu, 339
 - rpki::up_down::issue_pdu, 342
 - rpki::xml_utils::base_elt, 395
 - rpki::xml_utils::data_elt, 398
 - rpki::xml_utils::msg, 402
 - rpki::xml_utils::sax_handler, 405
 - rpki::xml_utils::text_elt, 408
- endElementNS
 - rpki::xml_utils::sax_handler, 405
- enforce_strict_up_down_xml_sender
 - rpki::left_right, 73
- err
 - rpki::async::sync_wrapper, 126
- errback
 - rpki::async::timer, 129, 131
 - rpki::https::http_request, 165
- error
 - rpki::log, 76
- error_code
 - rpki::left_right::report_error_elt, 206
 - rpki::publication::report_error_elt, 242
- error_text
 - rpki::left_right::report_error_elt, 207
 - rpki::publication::report_error_elt, 242
- event_loop
 - rpki::async, 64
- Exception, 95
- exceptions
 - rpki::up_down::error_response_pdu, 340
- exceptions.py(2742), 410
- excludes
 - irbe_cli::bsc_elt, 96
 - irbe_cli::cmd_elt_mixin, 103
 - irbe_cli::list_published_objects_elt, 108
- execute
 - rpki::sql::session, 310
- executemany
 - rpki::sql::session, 310
- exit_event_loop
 - rpki::async, 64
- ExitNow
 - rpki::async, 65
- expect_close
 - rpki::https::http_client, 155
 - rpki::https::http_server, 169
- expired
 - rpki::x509::X509, 387
- expires
 - rpki::rpki_engine::revoked_cert_obj, 295
- explicitVersion
 - rpki::manifest::Manifest, 223
 - rpki::roa::RouteOriginAttestation, 276
- extract
 - rpki::x509::CMS_object, 357
- fetch
 - rpki::publication::config_elt, 230
 - rpki::rpki_engine::child_cert_obj, 291
- fetch_active
 - rpki::rpki_engine::ca_obj, 286
- fetch_deprecated
 - rpki::rpki_engine::ca_obj, 287
- fetch_nonnull_nonrevoked
 - rpki::rpki_engine::ca_obj, 287
- fetch_pending
 - rpki::rpki_engine::ca_obj, 287
- fetch_revoked
 - rpki::rpki_engine::ca_obj, 287
- fetchall
 - rpki::sql::session, 310
- file

- rpki::manifest::FileAndHash, 221
- fileHashAlg
 - rpki::manifest::Manifest, 223
- fileList
 - rpki::manifest::Manifest, 223
- filename
 - rpki::config::parser, 134
- find_handler
 - rpki::https::http_server, 168
- format
 - rpki::https::http_message, 160
- format_first_line
 - rpki::https::http_request, 165
 - rpki::https::http_response, 166
- formats
 - rpki::x509::CMS_object, 359
 - rpki::x509::CRL, 363
 - rpki::x509::DER_object, 371
 - rpki::x509::PKCS10, 376
 - rpki::x509::RSA, 380
 - rpki::x509::RSAPublic, 383
 - rpki::x509::X509, 389
- found_terminator
 - rpki::https::http_stream, 172
- from_bytes
 - rpki::ipaddr::v4addr, 177
 - rpki::ipaddr::v6addr, 179
- from_exception
 - rpki::left_right::report_error_elt, 206
 - rpki::publication::report_error_elt, 241
- from_resource_bag
 - rpki::up_down::class_elt, 334
- from_rfc3779_tuples
 - rpki::resource_set::resource_bag, 246
- from_sql
 - rpki::resource_set::resource_set, 256
 - rpki::resource_set::roa_prefix_set, 268
 - rpki::sundial::datetime, 321
 - rpki::x509::DER_object, 367
- fromASN1tuple
 - rpki::sundial::datetime, 322
- fromdatetime
 - rpki::sundial::datetime, 322
- fromGeneralizedTime
 - rpki::sundial::datetime, 322
- fromtimedelta
 - rpki::sundial::timedelta, 327
- fromUTCTime
 - rpki::sundial::datetime, 322
- fromXMLtime
 - rpki::sundial::datetime, 322
- func
 - rpki::async::sync_wrapper, 126
- gAKI
 - rpki::x509::DER_object, 367
- gctx
 - rpki::rpki_engine::ca_detail_obj, 282
 - rpki::rpki_engine::ca_obj, 289
 - rpki::rpki_engine::child_cert_obj, 293
 - rpki::rpki_engine::revoked_cert_obj, 295
 - rpki::rpki_engine::roa_obj, 300
 - rpki::sql::sql_persistent, 317
- generate
 - rpki::rpki_engine::roa_obj, 298
 - rpki::x509::CRL, 361
 - rpki::x509::RSA, 379
- generate_crl
 - rpki::rpki_engine::ca_detail_obj, 279
- generate_manifest
 - rpki::rpki_engine::ca_detail_obj, 279
- generate_manifest_cert
 - rpki::rpki_engine::ca_detail_obj, 279
- get
 - rpki::config::parser, 132
- get_3779resources
 - rpki::x509::DER_object, 368
- get_AIA
 - rpki::x509::DER_object, 368
- get_AKI
 - rpki::x509::DER_object, 368
- get_Base64
 - rpki::x509::DER_object, 368

- get_basicConstraints
 - rpki::x509::DER_object, 368
- get_buffer
 - rpki::https::http_stream, 173
- get_content
 - rpki::x509::CMS_object, 357
- get_DER
 - rpki::x509::CMS_object, 357
 - rpki::x509::CRL, 361
 - rpki::x509::DER_object, 369
 - rpki::x509::PKCS10, 375
 - rpki::x509::RSA, 379
 - rpki::x509::RSAPublic, 382
 - rpki::x509::X509, 387
- get_PEM
 - rpki::x509::DER_object, 369
- get_POW
 - rpki::x509::CMS_object, 357
 - rpki::x509::CRL, 362
 - rpki::x509::RSA, 379
 - rpki::x509::RSAPublic, 382
 - rpki::x509::X509, 387
- get_POWpkix
 - rpki::x509::CRL, 362
 - rpki::x509::PKCS10, 375
 - rpki::x509::X509, 387
- get_public_DER
 - rpki::x509::RSA, 380
- get_root_cert
 - rootd, 57
- get_RSAPublic
 - rpki::x509::RSA, 380
- get_SIA
 - rpki::x509::DER_object, 369
- get_SKI
 - rpki::up_down::revoke_pdu, 351
 - rpki::x509::DER_object, 369
 - rpki::x509::RSA, 380
 - rpki::x509::RSAPublic, 382
- get_subject_cert
 - rootd, 58
- get_subject_pkcs10
 - rootd, 58
- getboolean
 - rpki::config::parser, 133
- getint
 - rpki::config::parser, 133
- getIssuer
 - rpki::x509::CRL, 362
 - rpki::x509::X509, 387
- getNextUpdate
 - rpki::x509::CRL, 362
 - rpki::x509::SignedManifest, 384
- getNotAfter
 - rpki::x509::X509, 388
- getNotBefore
 - rpki::x509::X509, 388
- getPublicKey
 - rpki::x509::PKCS10, 376
 - rpki::x509::X509, 388
- getSerial
 - rpki::x509::X509, 388
- getSubject
 - rpki::x509::X509, 388
- getThisUpdate
 - rpki::x509::CRL, 362
 - rpki::x509::SignedManifest, 384
- gSKI
 - rpki::x509::DER_object, 370
- hAKI
 - rpki::x509::DER_object, 370
- handle_accept
 - rpki::https::http_listener, 158
- handle_body
 - rpki::https::http_stream, 173
- handle_close
 - rpki::https::http_client, 153
 - rpki::https::http_stream, 173
- handle_connect
 - rpki::https::http_client, 154
- handle_dispatch
 - irdbd, 52
- handle_error
 - rpki::https::http_client, 154
 - rpki::https::http_listener, 158
 - rpki::https::http_stream, 173
- handle_list_resources
 - irdbd, 50
- handle_list_roa_requests
 - irdbd, 50
- handle_message

- rpki::https::http_client, 154
- rpki::https::http_server, 168
- handle_no_content_length
 - rpki::https::http_client, 154
 - rpki::https::http_server, 168
- handle_read
 - rpki::https::http_stream, 173
- handle_timeout
 - rpki::https::http_client, 154
 - rpki::https::http_stream, 173
- handle_write
 - rpki::https::http_stream, 173
- handler
 - irdbd, 50
 - rpki::async::timer, 129, 131
- handler_common
 - pubd::pubd_context, 116
- handlers
 - irdbd, 52
 - rootd, 59
 - rpki::https::http_listener, 158
 - rpki::https::http_server, 169
- handles
 - rpki::left_right::bsc_elt, 182
 - rpki::left_right::child_elt, 187
 - rpki::left_right::data_elt, 191
 - rpki::left_right::parent_elt, 204
 - rpki::left_right::repository_elt, 210
 - rpki::left_right::self_elt, 218
- has_option
 - rpki::config::parser, 133
- has_section
 - rpki::config::parser, 133
- hash
 - rpki::manifest::FileAndHash, 221
- headers
 - rpki::https::http_message, 161
- host
 - irdbd, 52
 - rootd, 59
- hostport
 - rpki::https::http_client, 155
 - rpki::https::http_queue, 163
- hSKI
 - rpki::x509::DER_object, 370
- https.py(2751), 412
- https_server_host
 - pubd::pubd_context, 116
 - rootd, 60
 - rpki::rpki_engine::rpkid_context, 306
- https_server_port
 - pubd::pubd_context, 116
 - rootd, 60
 - rpki::rpki_engine::rpkid_context, 306
- https_ta_cache
 - pubd::pubd_context, 117
 - rpki::rpki_engine::rpkid_context, 306
- ignore
 - rpki::async::iterator, 124
- index
 - rpki::sql::template, 319
- info
 - rpki::log, 76
- inherit
 - rpki::resource_set::resource_set, 258
 - rpki::resource_set::resource_set_as, 259
 - rpki::resource_set::resource_set_ip, 261
- inherit_token
 - rpki::resource_set, 84
- init
 - rpki::log, 75
- initial_delay
 - rpki::rpki_engine::rpkid_context, 306
- initiate_send
 - rpki::https::http_stream, 174
- insert
 - rpki::sql::template, 319
- intersection
 - rpki::resource_set::resource_bag, 246
 - rpki::resource_set::resource_set, 256
- ipAddrBlocks
 - rpki::roa::RouteOriginAttestation, 276
- ipaddrs.py(2424), 413

- ipv4
 - rpki::left_right::list_resources_elt, 196
 - rpki::left_right::list_roa_requests_elt, 198
 - rpki::rpki_engine::roa_obj, 301
- ipv6
 - rpki::left_right::list_resources_elt, 197
 - rpki::left_right::list_roa_requests_elt, 198
 - rpki::rpki_engine::roa_obj, 301
- irbe_cert
 - pubd::pubd_context, 117
 - rpki::rpki_engine::rpkiid_context, 306
- irbe_cli, 45
 - argv, 47
 - call_pubd, 47
 - call_rpkid, 47
 - cfg, 47
 - cfg_file, 47
 - pem_out, 48
 - q_msg, 48
 - q_msg_left_right, 48
 - q_msg_publication, 48
 - q_pdu, 48
 - top_opts, 48
 - usage, 46
 - usage_fill, 48
 - verbose, 49
- irbe_cli.py(2799), 413
- irbe_cli::bsc_elt, 95
 - client_query_signing_cert, 96
 - client_query_signing_cert_crl, 96
 - client_reply_decode, 96
 - excludes, 96
 - signing_cert, 96
 - signing_cert_crl, 96
- irbe_cli::caller, 97
 - __call__, 97
 - __init__, 97
 - client_cert, 98
 - client_key, 98
 - cms_class, 98
 - server_cert, 98
 - server_ta, 98
 - url, 98
- irbe_cli::certificate_elt, 99
- irbe_cli::child_elt, 99
- irbe_cli::client_elt, 99
- irbe_cli::cmd_elt_mixin, 99
 - bpki_cert, 102
 - bpki_cms_cert, 102
 - bpki_cms_glue, 102
 - bpki_glue, 102
 - bpki_https_cert, 103
 - bpki_https_glue, 103
 - client_getopt, 101
 - client_query_bpki_cert, 101
 - client_query_bpki_cms_cert, 101
 - client_query_bpki_https_cert, 101
 - client_query_cms_glue, 101
 - client_query_glue, 101
 - client_query_https_glue, 102
 - excludes, 103
 - is_cmd, 103
 - usage, 102
- irbe_cli::cmd_msg_mixin, 103
 - usage, 104
- irbe_cli::config_elt, 104
 - bpki_crl, 105
 - client_query_bpki_crl, 105
- irbe_cli::crl_elt, 105
- irbe_cli::left_right_cms_msg, 105
 - saxify, 106
- irbe_cli::left_right_msg, 106
 - pdu, 106
- irbe_cli::left_right_sax_handler, 107
 - pdu, 107
- irbe_cli::list_published_objects_elt, 107
 - excludes, 108
- irbe_cli::manifest_elt, 108
- irbe_cli::parent_elt, 108
- irbe_cli::publication_cms_msg, 109
 - saxify, 109
- irbe_cli::publication_msg, 109
 - pdu, 110
- irbe_cli::publication_sax_handler, 110
 - pdu, 110
- irbe_cli::reply_elt_mixin, 111
 - client_reply_decode, 111

- client_reply_show, 111
- is_cmd, 111
- irbe_cli::report_error_elt, 112
- irbe_cli::repository_elt, 112
- irbe_cli::roa_elt, 112
- irbe_cli::self_elt, 113
- irbe_cli::UsageWrapper, 113
 - __call__, 113
- irdb_cert
 - rpki::rpki_engine::rpkid_context, 306
- irdb_query
 - rpki::rpki_engine::rpkid_context, 304
- irdb_query_child_resources
 - rpki::rpki_engine::rpkid_context, 304
- irdb_query_roa_requests
 - rpki::rpki_engine::rpkid_context, 304
- irdb_url
 - rpki::rpki_engine::rpkid_context, 306
- irdbd, 49
 - bpki_ta, 51
 - cfg, 51
 - cfg_file, 51
 - client_ta, 51
 - cur, 51
 - db, 51
 - handle_dispatch, 52
 - handle_list_resources, 50
 - handle_list_roa_requests, 50
 - handler, 50
 - handlers, 52
 - host, 52
 - irdbd_cert, 52
 - irdbd_key, 52
 - port, 52
 - rpkid_cert, 53
 - server_cert, 53
 - startup_msg, 53
 - u, 53
- irdbd.py(2799), 414
- irdbd_cert
 - irdbd, 52
- irdbd_key
 - irdbd, 52
- is_CA
 - rpki::x509::DER_object, 370
- is_cmd
 - irbe_cli::cmd_elt_mixin, 103
 - irbe_cli::reply_elt_mixin, 111
- is_query
 - rpki::xml_utils::msg, 402
- is_reply
 - rpki::xml_utils::msg, 402
- is_set
 - rpki::async::timer, 129
- issubset
 - rpki::resource_set::resource_set, 257
- issue
 - rpki::rpki_engine::ca_detail_obj, 280
 - rpki::x509::X509, 389
- issue_ee
 - rpki::rpki_engine::ca_detail_obj, 280
- issue_subject_cert_maybe
 - rootd, 58
- issuer
 - rpki::up_down::class_elt, 335
- issuperset
 - rpki::resource_set::resource_set, 257
- item_callback
 - rpki::async::iterator, 124
- iterator
 - rpki::async::iterator, 124
- key
 - rpki::https::http_client, 155
 - rpki::https::http_listener, 158
 - rpki::https::http_queue, 163
- last_crl_sn
 - rpki::rpki_engine::ca_obj, 289
- last_issued_sn
 - rpki::rpki_engine::ca_obj, 289
- last_manifest_sn
 - rpki::rpki_engine::ca_obj, 289
- lastrowid
 - rpki::sql::session, 310

- later
 - rpki::sundial::datetime, [322](#)
- latest_ca_cert
 - rpki::rpki_engine::ca_detail_obj, [282](#)
- latest_crl
 - rpki::rpki_engine::ca_detail_obj, [282](#)
- latest_manifest
 - rpki::rpki_engine::ca_detail_obj, [282](#)
- latest_manifest_cert
 - rpki::rpki_engine::ca_detail_obj, [283](#)
- left_right
 - rpki::relaxng, [81](#)
- left_right.py(2795), [415](#)
- left_right_handler
 - rpki::rpki_engine::rpkid_context, [304](#)
- log
 - rpki::https::http_listener, [158](#)
 - rpki::https::http_queue, [163](#)
 - rpki::https::http_stream, [175](#)
- log.py(2732), [416](#)
- log_cert
 - rpki::https::http_stream, [174](#)
- log_query
 - rootd::message_pdu, [120](#)
 - rpki::up_down::message_pdu, [347](#)
- logger
 - rpki::https, [69](#)
- long, [114](#)
- looks_like_PEM
 - rpki::x509::PEM_converter, [373](#)
- main
 - pubd, [54](#)
 - rpkid, [94](#)
- make_b64elt
 - rpki::up_down::base_elt, [329](#)
 - rpki::xml_utils::base_elt, [395](#)
- make_elt
 - rpki::up_down::base_elt, [329](#)
 - rpki::xml_utils::base_elt, [395](#)
- make_pdu
 - rpki::xml_utils::base_elt, [395](#)
- make_prefix
 - rpki::resource_set::resource_range_ip, [252](#)
- make_publish
 - rpki::publication::publication_object_elt, [238](#)
- make_query
 - rpki::up_down::message_pdu, [347](#)
- make_reply
 - rpki::left_right::list_published_objects_elt, [193](#)
 - rpki::xml_utils::data_elt, [398](#)
- make_reply_clone_hook
 - rpki::left_right::data_elt, [189](#)
 - rpki::xml_utils::data_elt, [398](#)
- make_withdraw
 - rpki::publication::publication_object_elt, [238](#)
- manifest.py(2424), [417](#)
- manifest_private_key_id
 - rpki::rpki_engine::ca_detail_obj, [283](#)
- manifest_public_key
 - rpki::rpki_engine::ca_detail_obj, [283](#)
- manifest_uri
 - rpki::rpki_engine::ca_detail_obj, [280](#)
- manifestNumber
 - rpki::manifest::Manifest, [223](#)
- map
 - rpki::sql::template, [319](#)
- max
 - rpki::resource_set::resource_range, [249](#)
 - rpki::resource_set::roa_prefix, [265](#)
- max_prefixlen
 - rpki::resource_set::roa_prefix, [266](#)
- maxLength
 - rpki::roa::ROAIPAddress, [272](#)
- min
 - rpki::resource_set::resource_range, [249](#)
 - rpki::resource_set::resource_range_as, [251](#)

- rpki::resource_set::roa_prefix, 265
- msg
 - rpki::https::http_stream, 175
- multiget
 - rpki::config::parser, 133
- name
 - rpki::left_right::sax_handler, 211
 - rpki::publication::sax_handler, 244
 - rpki::up_down::sax_handler, 355
- name2oid
 - rpki::oids, 78
- name2type
 - rootd::message_pdu, 121
 - rpki::up_down::message_pdu, 348
- next_crl_number
 - rpki::rpki_engine::ca_obj, 287
- next_manifest_number
 - rpki::rpki_engine::ca_obj, 288
- next_serial_number
 - rpki::rpki_engine::ca_obj, 288
- nextUpdate
 - rpki::manifest::Manifest, 223
 - rpki::rpki_engine::ca_detail_obj, 283
- normalize_chain
 - rpki::x509::X509, 389
- normalize_headers
 - rpki::https::http_message, 160
- note
 - rpki::log, 76
- now
 - rpki::sundial, 88
- nsmap
 - rpki::left_right::left_right_namespace, 192
 - rpki::publication::publication_namespace, 237
 - rpki::up_down, 90
- obj
 - rpki::left_right::list_published_objects_elt, 194
- object, 114
- oid2name
 - rpki::oids, 79
- oids.py(2424), 417
- other_clear
 - rpki::x509::CMS_object, 359
 - rpki::x509::DER_object, 371
- oversized
 - rpki::resource_set::resource_bag, 247
- parent
 - rpki::rpki_engine::ca_obj, 288
- parent_id
 - rpki::rpki_engine::ca_obj, 289
- parent_resource_class
 - rpki::rpki_engine::ca_obj, 289
- parents
 - rpki::left_right::bsc_elt, 180
 - rpki::left_right::child_elt, 185
 - rpki::left_right::repository_elt, 208
 - rpki::left_right::self_elt, 214
- parse
 - rpki::sundial::timedelta, 327
- parse_first_line
 - rpki::https::http_request, 165
 - rpki::https::http_response, 167
- parse_from_wire
 - rpki::https::http_message, 160
- parse_rfc3779_tuple
 - rpki::resource_set::resource_set_as, 259
 - rpki::resource_set::resource_set_ip, 260
- parse_str
 - rpki::resource_set::resource_set_as, 259
 - rpki::resource_set::resource_set_ip, 260
 - rpki::resource_set::roa_prefix_set, 269
- parse_type
 - rpki::https::http_client, 155
 - rpki::https::http_server, 169
- parse_version
 - rpki::https::http_message, 160
- password
 - rpki::sql::session, 311
- path

- rpki::https::http_request, 165
- payload
 - rpki::publication::publication_ - object_elt, 240
 - rpki::up_down::message_pdu, 349
- payload_type
 - rpki::publication::certificate_elt, 224
 - rpki::publication::crl_elt, 233
 - rpki::publication::manifest_elt, 234
 - rpki::publication::publication_ - object_elt, 240
 - rpki::publication::roa_elt, 243
- pdu
 - irbe_cli::left_right_sax_handler, 107
 - irbe_cli::publication_sax_handler, 110
 - rootd::sax_handler, 122
 - rpki::left_right::sax_handler, 211
 - rpki::publication::sax_handler, 244
 - rpki::up_down::sax_handler, 355
- pdus
 - irbe_cli::left_right_msg, 106
 - irbe_cli::publication_msg, 110
 - rpki::left_right::msg, 200
 - rpki::publication::msg, 236
- pem_converter
 - rpki::x509::CMS_object, 359
 - rpki::x509::CRL, 363
 - rpki::x509::DER_object, 372
 - rpki::x509::PKCS10, 376
 - rpki::x509::ROA, 378
 - rpki::x509::RSA, 381
 - rpki::x509::RSAPublic, 383
 - rpki::x509::SignedManifest, 385
 - rpki::x509::X509, 390
- pem_out
 - irbe_cli, 48
- persistent
 - rpki::https::http_message, 160
- pid
 - rpki::log, 76
- ping
 - rpki::sql::session, 310
- pkcs10
 - rpki::up_down::issue_pdu, 343
- pkcs10_request
 - rpki::left_right::bsc_elt, 182
- PKIX_threshold
 - rpki::sundial::datetime, 324
- port
 - irdbd, 52
 - rootd, 60
- POW
 - rpki::x509::CMS_object, 360
 - rpki::x509::CRL, 363
 - rpki::x509::RSA, 381
 - rpki::x509::RSAPublic, 383
 - rpki::x509::X509, 390
- POWify_OID
 - rpki::x509, 92
- POWpkix
 - rpki::x509::CRL, 363
 - rpki::x509::PKCS10, 377
 - rpki::x509::X509, 390
- prefix
 - rpki::resource_set::roa_prefix, 266
- prefix_type
 - rpki::resource_set::roa_prefix_set_ - ipv4, 270
 - rpki::resource_set::roa_prefix_set_ - ipv6, 271
- prefixlen
 - rpki::resource_set::roa_prefix, 266
- pretty_print_content
 - rpki::x509::XML_CMS_object, 392
- print_on_der_error
 - rpki::x509::CMS_object, 360
- priority
 - rpki::log::logger, 220
- private_key_id
 - rpki::left_right::bsc_elt, 182
 - rpki::rpki_engine::ca_detail_obj, 283
- profile
 - pubd, 55
 - rpkid, 94
- pubd, 53
 - cfg_file, 55
 - main, 54
 - profile, 55
- pubd.py(2799), 417
- pubd::pubd_context, 114

- [__init__, 115](#)
 - [bpki_ta, 116](#)
 - [build_https_ta_cache, 115](#)
 - [clear_https_ta_cache, 115](#)
 - [client_handler, 115](#)
 - [client_url_regexp, 116](#)
 - [control_handler, 116](#)
 - [handler_common, 116](#)
 - [https_server_host, 116](#)
 - [https_server_port, 116](#)
 - [https_ta_cache, 117](#)
 - [irbe_cert, 117](#)
 - [pubd_cert, 117](#)
 - [pubd_key, 117](#)
 - [publication_base, 117](#)
 - [sql, 117](#)
- [pubd_cert](#)
 - [pubd::pubd_context, 117](#)
- [pubd_key](#)
 - [pubd::pubd_context, 117](#)
- [public_key](#)
 - [rpki::rpki_engine::ca_detail_obj, 283](#)
- [publication](#)
 - [rpki::relaxng, 81](#)
- [publication.py\(2798\), 418](#)
- [publication_base](#)
 - [pubd::pubd_context, 117](#)
- [publication_kludge_base](#)
 - [rpki::rpki_engine::rpkid_context, 307](#)
- [publish](#)
 - [rpki::left_right::repository_elt, 209](#)
- [pydatetime::datetime, 118](#)
- [pydatetime::timedelta, 118](#)
- [q_msg](#)
 - [irbe_cli, 48](#)
- [q_msg_left_right](#)
 - [irbe_cli, 48](#)
- [q_msg_publication](#)
 - [irbe_cli, 48](#)
- [q_pdu](#)
 - [irbe_cli, 48](#)
- [query](#)
 - [rpki::up_down::issue_pdu, 342](#)
 - [rpki::up_down::list_pdu, 345](#)
 - [rpki::up_down::revoke_pdu, 351](#)
 - [rpki::xml_utils::msg, 402](#)
- [query_up_down](#)
 - [rpki::left_right::parent_elt, 201](#)
- [queue](#)
 - [rpki::async::timer, 131](#)
 - [rpki::https::http_client, 156](#)
 - [rpki::https::http_queue, 163](#)
- [range_type](#)
 - [rpki::resource_set::resource_set_as, 259](#)
 - [rpki::resource_set::resource_set_ipv4, 262](#)
 - [rpki::resource_set::resource_set_ipv6, 263](#)
 - [rpki::resource_set::roa_prefix_ipv4, 267](#)
 - [rpki::resource_set::roa_prefix_ipv6, 267](#)
- [read_attrs](#)
 - [rpki::xml_utils::base_elt, 395](#)
- [readable](#)
 - [rpki::https::http_stream, 174](#)
- [reason](#)
 - [rpki::https::http_response, 167](#)
- [recipient](#)
 - [rpki::up_down::message_pdu, 349](#)
- [recv](#)
 - [rpki::https::http_stream, 174](#)
- [regen_margin](#)
 - [rpki::left_right::self_elt, 219](#)
- [regenerate](#)
 - [rpki::rpki_engine::roa_obj, 298](#)
- [regenerate_crls_and_manifests](#)
 - [rpki::left_right::self_elt, 214](#)
- [regexp](#)
 - [rpki::sundial::timedelta, 328](#)
- [reissue](#)
 - [rpki::rpki_engine::child_cert_obj, 292](#)
- [rekey](#)
 - [rpki::rpki_engine::ca_obj, 288](#)
- [relaxng.py\(2794\), 418](#)
- [reply](#)

- rpki::xml_utils::msg, 403
- repositories
 - rpki::left_right::bsc_elt, 181
 - rpki::left_right::self_elt, 214
- repository
 - rpki::left_right::parent_elt, 202
- req_resource_set_as
 - rpki::up_down::certificate_elt, 332
 - rpki::up_down::issue_pdu, 343
- req_resource_set_ipv4
 - rpki::up_down::certificate_elt, 332
 - rpki::up_down::issue_pdu, 343
- req_resource_set_ipv6
 - rpki::up_down::certificate_elt, 332
 - rpki::up_down::issue_pdu, 343
- request
 - rpki::https::http_queue, 162
- require_crls
 - rpki::x509::CMS_object, 360
- res
 - rpki::async::sync_wrapper, 126
- resource_set.py(2776), 419
- resource_set_as
 - rpki::up_down::class_elt, 335
- resource_set_ipv4
 - rpki::up_down::class_elt, 335
- resource_set_ipv6
 - rpki::up_down::class_elt, 335
- resource_set_notafter
 - rpki::up_down::class_elt, 335
- resource_set_type
 - rpki::resource_set::roa_prefix_set_ipv4, 270
 - rpki::resource_set::roa_prefix_set_ipv6, 271
- restart
 - rpki::https::http_queue, 162
 - rpki::https::http_stream, 174
- result
 - rpki::xml_utils::sax_handler, 407
- retried
 - rpki::https::http_request, 166
- retry_read
 - rpki::https::http_client, 156
 - rpki::https::http_server, 170
 - rpki::https::http_stream, 175
- retry_write
 - rpki::https::http_client, 156
 - rpki::https::http_server, 170
 - rpki::https::http_stream, 175
- return_result
 - rpki::https::http_queue, 162
- revoke
 - rpki::rpki_engine::ca_detail_obj, 280
 - rpki::rpki_engine::ca_obj, 288
 - rpki::rpki_engine::child_cert_obj, 292
 - rpki::rpki_engine::revoked_cert_obj, 295
 - rpki::rpki_engine::roa_obj, 298
- revoked
 - rpki::rpki_engine::revoked_cert_obj, 296
- revoked_certs
 - rpki::rpki_engine::ca_detail_obj, 281
- roa
 - rpki::rpki_engine::roa_obj, 301
- roa.py(2424), 420
- roas
 - rpki::left_right::self_elt, 214
 - rpki::rpki_engine::ca_detail_obj, 281
- root_newer_than_subject
 - rootd, 58
- rootd, 55
 - bpki_ta, 59
 - cfg, 59
 - cfg_file, 59
 - child_bpki_cert, 59
 - client_ta, 59
 - compose_response, 57
 - del_subject_cert, 57
 - del_subject_pkcs10, 57
 - get_root_cert, 57
 - get_subject_cert, 58
 - get_subject_pkcs10, 58
 - handlers, 59
 - host, 59
 - https_server_host, 60
 - https_server_port, 60

- issue_subject_cert_maybe, 58
- port, 60
- root_newer_than_subject, 58
- rootd_bpki_cert, 60
- rootd_bpki_crl, 60
- rootd_bpki_key, 60
- rpki_base_uri, 60
- rpki_class_name, 61
- rpki_root_cert, 61
- rpki_root_cert_file, 61
- rpki_root_cert_uri, 61
- rpki_root_crl, 61
- rpki_root_dir, 61
- rpki_root_key, 61
- rpki_root_manifest, 62
- rpki_subject_cert, 62
- rpki_subject_lifetime, 62
- rpki_subject_pkcs10, 62
- rpki_subject_regen, 62
- server_cert, 62
- set_subject_cert, 58
- set_subject_pkcs10, 58
- up_down_handler, 58
- rootd.py(2810), 420
- rootd::cms_msg, 118
 - saxify, 118
- rootd::issue_pdu, 119
 - serve_pdu, 119
- rootd::list_pdu, 119
 - serve_pdu, 120
- rootd::message_pdu, 120
 - log_query, 120
 - name2type, 121
 - type2name, 121
- rootd::revoke_pdu, 121
 - serve_pdu, 122
- rootd::sax_handler, 122
 - pdu, 122
- rootd_bpki_cert
 - rootd, 60
- rootd_bpki_crl
 - rootd, 60
- rootd_bpki_key
 - rootd, 60
- rpki, 63
- rpki.async, 63
 - rpki.config, 65
 - rpki.exceptions, 66
 - rpki.https, 68
 - rpki.ipaddrs, 71
 - rpki.left_right, 72
 - rpki.log, 74
 - rpki.manifest, 77
 - rpki.oids, 78
 - rpki.publication, 79
 - rpki.relaxng, 80
 - rpki.resource_set, 81
 - rpki.roa, 84
 - rpki.rpki_engine, 85
 - rpki.sql, 86
 - rpki.sundial, 87
 - rpki.up_down, 89
 - rpki.x509, 90
 - rpki.xml_utils, 92
 - rpki::async
 - _raiseExitNow, 64
 - event_loop, 64
 - exit_event_loop, 64
 - ExitNow, 65
 - rpki::async::iterator, 122
 - _call_, 123
 - _init_, 123
 - _repr_, 124
 - caller_function, 124
 - doit, 124
 - done_callback, 124
 - ignore, 124
 - item_callback, 124
 - iterator, 124
 - timer, 125
 - rpki::async::sync_wrapper, 125
 - _call_, 126
 - _init_, 126
 - cb, 126
 - eb, 126
 - err, 126
 - func, 126
 - res, 126
 - rpki::async::timer, 127
 - _cmp_, 128
 - _init_, 128
 - _repr_, 128

- cancel, 128
- clear, 128
- errback, 129, 131
- handler, 129, 131
- is_set, 129
- queue, 131
- runq, 129
- seconds_until_wakeup, 129
- set, 130
- set_errback, 130
- set_handler, 130
- when, 131
- rpki::config::parser, 131
 - __init__, 132
 - _get_wrapper, 132
 - cfg, 134
 - default_section, 134
 - filename, 134
 - get, 132
 - getboolean, 133
 - getint, 133
 - has_option, 133
 - has_section, 133
 - multiget, 133
- rpki::exceptions::BadClassNameSyntax, 134
- rpki::exceptions::BadClientURL, 135
- rpki::exceptions::BadContactURL, 135
- rpki::exceptions::BadExtension, 135
- rpki::exceptions::BadIRDBReply, 136
- rpki::exceptions::BadIssueResponse, 136
- rpki::exceptions::BadPKCS10, 136
- rpki::exceptions::BadPublicationReply, 137
- rpki::exceptions::BadQuery, 137
- rpki::exceptions::BadSender, 137
- rpki::exceptions::BadStatusCode, 138
- rpki::exceptions::BadURISyntax, 138
- rpki::exceptions::BSCNotFound, 138
- rpki::exceptions::BSCNotReady, 139
- rpki::exceptions::ChildNotFound, 139
- rpki::exceptions::ClassNameMismatch, 139
- rpki::exceptions::ClassNameUnknown, 140
- rpki::exceptions::ClientNotFound, 140
- rpki::exceptions::CMSCRLNotSet, 140
- rpki::exceptions::CMSVerificationFailed, 141
- rpki::exceptions::DBConsistencyError, 141
- rpki::exceptions::DERObjectConversionError, 141
- rpki::exceptions::DuplicateObject, 142
- rpki::exceptions::EmptyPEM, 142
- rpki::exceptions::EmptyROAPrefixList, 142
- rpki::exceptions::ForbiddenURI, 143
- rpki::exceptions::HandleTranslationError, 143
- rpki::exceptions::HTTPRequestFailed, 143
- rpki::exceptions::HTTPSBadVersion, 144
- rpki::exceptions::HTTPSClientAborted, 144
- rpki::exceptions::HTTPSUnexpectedState, 144
- rpki::exceptions::MissingCMSCRL, 145
- rpki::exceptions::MissingCMSEECert, 145
- rpki::exceptions::MultipleTLSEECert, 145
- rpki::exceptions::MustBePrefix, 146
- rpki::exceptions::NoActiveCA, 146
- rpki::exceptions::NoCoveringCertForROA, 146
- rpki::exceptions::NoObjectAtURI, 147
- rpki::exceptions::NotACertificateChain, 147
- rpki::exceptions::NotFound, 147
- rpki::exceptions::NotImplementedYet, 148
- rpki::exceptions::NotInDatabase, 148
- rpki::exceptions::ReceivedTLSCACert, 148
- rpki::exceptions::RPKI_Exception, 149
- rpki::exceptions::ServerShuttingDown, 149
- rpki::exceptions::SKIMismatch, 150
- rpki::exceptions::SubprocessError, 150
- rpki::exceptions::TLSValidationError, 150

- rpki::exceptions::UnexpectedCMSCerts, 151
- rpki::exceptions::UnexpectedCMSCRLs, 151
- rpki::exceptions::UnparsableCMSDER, 151
- rpki::exceptions::UpstreamError, 152
- rpki::exceptions::WrongEContentType, 152
- rpki::https
 - build_https_ta_cache, 69
 - client, 69
 - client_queues, 70
 - debug_http, 70
 - debug_tls_certs, 70
 - default_client_timeout, 70
 - default_http_version, 70
 - default_server_timeout, 71
 - logger, 69
 - rpki_content_type, 71
 - server, 70
 - want_persistent_client, 71
 - want_persistent_server, 71
- rpki::https::http_client, 152
 - __init__, 153
 - cert, 155
 - expect_close, 155
 - handle_close, 153
 - handle_connect, 154
 - handle_error, 154
 - handle_message, 154
 - handle_no_content_length, 154
 - handle_timeout, 154
 - hostport, 155
 - key, 155
 - parse_type, 155
 - queue, 156
 - retry_read, 156
 - retry_write, 156
 - send_request, 154
 - set_state, 154
 - start, 155
 - state, 156
 - ta, 156
 - timeout, 156
 - tls, 156
 - tls_connect, 155
- rpki::https::http_listener, 157
 - __init__, 157
 - cert, 158
 - dynamic_ta, 158
 - handle_accept, 158
 - handle_error, 158
 - handlers, 158
 - key, 158
 - log, 158
 - ta, 158
- rpki::https::http_message, 159
 - __init__, 160
 - __str__, 160
 - body, 161
 - format, 160
 - headers, 161
 - normalize_headers, 160
 - parse_from_wire, 160
 - parse_version, 160
 - persistent, 160
 - software_name, 161
 - version, 161
- rpki::https::http_queue, 161
 - __init__, 162
 - cert, 163
 - client, 163
 - detach, 162
 - hostport, 163
 - key, 163
 - log, 163
 - queue, 163
 - request, 162
 - restart, 162
 - return_result, 162
 - send_request, 163
 - ta, 164
- rpki::https::http_request, 164
 - __init__, 165
 - callback, 165
 - cmd, 165
 - errback, 165
 - format_first_line, 165
 - parse_first_line, 165
 - path, 165
 - retrieved, 166

- rpki::https::http_response, 166
 - __init__, 166
 - code, 167
 - format_first_line, 166
 - parse_first_line, 167
 - reason, 167
- rpki::https::http_server, 167
 - __init__, 168
 - expect_close, 169
 - find_handler, 168
 - handle_message, 168
 - handle_no_content_length, 168
 - handlers, 169
 - parse_type, 169
 - retry_read, 170
 - retry_write, 170
 - send_error, 169
 - send_message, 169
 - send_reply, 169
 - timeout, 170
 - tls, 170
 - tls_accept, 169
- rpki::https::http_stream, 170
 - __init__, 172
 - buffer, 175
 - chunk_body, 172
 - chunk_discard_crlf, 172
 - chunk_discard_trailer, 172
 - chunk_handler, 175
 - chunk_header, 172
 - close, 172
 - collect_incoming_data, 172
 - found_terminator, 172
 - get_buffer, 173
 - handle_body, 173
 - handle_close, 173
 - handle_error, 173
 - handle_read, 173
 - handle_timeout, 173
 - handle_write, 173
 - initiate_send, 174
 - log, 175
 - log_cert, 174
 - msg, 175
 - readable, 174
 - recv, 174
 - restart, 174
 - retry_read, 175
 - retry_write, 175
 - send, 174
 - timer, 176
 - tls, 176
 - update_timeout, 174
 - writable, 175
- rpki::ipaddr::v4addr, 176
 - __new__, 177
 - __str__, 177
 - bits, 177
 - from_bytes, 177
 - to_bytes, 177
- rpki::ipaddr::v6addr, 178
 - __new__, 178
 - __str__, 178
 - bits, 179
 - from_bytes, 179
 - to_bytes, 179
- rpki::left_right
 - enforce_strict_up_down_xml_
sender, 73
- rpki::left_right::bsc_elt, 179
 - attributes, 181
 - booleans, 181
 - children, 180
 - element_name, 182
 - elements, 182
 - handles, 182
 - parents, 180
 - pkcs10_request, 182
 - private_key_id, 182
 - repositories, 181
 - serve_pre_save_hook, 181
 - signing_cert, 182
 - signing_cert_crl, 183
 - sql_template, 183
- rpki::left_right::child_elt, 183
 - attributes, 186
 - booleans, 186
 - bpki_cert, 186
 - bpki_glue, 186
 - ca_from_class_name, 184
 - child_certs, 184
 - clear_https_ta_cache, 187

- element_name, 187
- elements, 187
- endElement, 185
- handles, 187
- parents, 185
- serve_destroy_hook, 185
- serve_post_save_hook, 185
- serve_up_down, 186
- sql_template, 187
- rpki::left_right::cms_msg, 188
 - encoding, 188
 - saxify, 188
 - schema, 188
- rpki::left_right::data_elt, 189
 - bsc, 189
 - handles, 191
 - make_reply_clone_hook, 189
 - self, 190
 - self_handle, 191
 - self_id, 191
 - serve_fetch_all, 190
 - serve_fetch_handle, 190
 - serve_fetch_one_maybe, 190
 - serve_pre_save_hook, 191
- rpki::left_right::left_right_namespace, 192
 - nsmmap, 192
 - xmlns, 192
- rpki::left_right::list_published_objects_elt, 193
 - attributes, 194
 - element_name, 194
 - make_reply, 193
 - obj, 194
 - serve_dispatch, 193
 - text_attribute, 194
- rpki::left_right::list_resources_elt, 195
 - asn, 196
 - attributes, 196
 - element_name, 196
 - ipv4, 196
 - ipv6, 197
 - startElement, 195
 - toXML, 196
 - valid_until, 197
- rpki::left_right::list_roa_requests_elt, 197
 - attributes, 198
 - element_name, 198
 - ipv4, 198
 - ipv6, 198
 - startElement, 198
- rpki::left_right::msg, 199
 - pdus, 200
 - serve_top_level, 199
 - version, 200
- rpki::left_right::parent_elt, 200
 - attributes, 203
 - booleans, 203
 - bpki_cms_cert, 203
 - bpki_cms_glue, 204
 - bpki_https_cert, 204
 - bpki_https_glue, 204
 - cas, 201
 - element_name, 204
 - elements, 204
 - handles, 204
 - query_up_down, 201
 - repository, 202
 - serve_post_save_hook, 202
 - serve_rekey, 202
 - serve_revoke, 202
 - serve_revoke_forgotten, 202
 - sql_template, 205
- rpki::left_right::report_error_elt, 205
 - attributes, 206
 - element_name, 206
 - error_code, 206
 - error_text, 207
 - from_exception, 206
 - self_handle, 207
 - tag, 207
 - text_attribute, 207
- rpki::left_right::repository_elt, 207
 - attributes, 209
 - bpki_cert, 209
 - bpki_glue, 209
 - call_pubd, 208
 - element_name, 210
 - elements, 210
 - handles, 210
 - parents, 208
 - publish, 209

- sql_template, 210
- withdraw, 209
- rpki::left_right::sax_handler, 211
 - name, 211
 - pdu, 211
 - version, 211
- rpki::left_right::self_elt, 212
 - attributes, 217
 - booleans, 217
 - bpki_cert, 218
 - bpki_glue, 218
 - bscs, 213
 - children, 213
 - client_poll, 213
 - crl_interval, 218
 - cron, 213
 - element_name, 218
 - elements, 218
 - handles, 218
 - parents, 214
 - regen_margin, 219
 - regenerate_crls_and_manifests, 214
 - repositories, 214
 - roas, 214
 - serve_fetch_all, 214
 - serve_fetch_handle, 215
 - serve_fetch_one_maybe, 215
 - serve_post_save_hook, 215
 - serve_publish_world_now, 215
 - serve_rekey, 216
 - serve_revoke, 216
 - serve_revoke_forgotten, 216
 - serve_run_now, 216
 - sql_template, 219
 - update_children, 217
 - update_roas, 217
 - use_hsm, 219
- rpki::log
 - debug, 76
 - enable_trace, 76
 - error, 76
 - info, 76
 - init, 75
 - note, 76
 - pid, 76
 - set_trace, 75
 - tag, 77
 - trace, 75
 - traceback, 75
 - use_syslog, 77
 - warn, 77
- rpki::log::logger, 219
 - __call__, 220
 - __init__, 220
 - priority, 220
- rpki::manifest::FileAndHash, 220
 - __init__, 221
 - file, 221
 - hash, 221
- rpki::manifest::FilesAndHashes, 221
 - __init__, 222
- rpki::manifest::Manifest, 222
 - __init__, 222
 - explicitVersion, 223
 - fileHashAlg, 223
 - fileList, 223
 - manifestNumber, 223
 - nextUpdate, 223
 - thisUpdate, 223
 - version, 223
- rpki::oids
 - name2oid, 78
 - oid2name, 79
- rpki::publication::certificate_elt, 224
 - element_name, 224
 - payload_type, 224
- rpki::publication::client_elt, 225
 - attributes, 227
 - base_uri, 227
 - bpki_cert, 227
 - bpki_glue, 227
 - check_allowed_uri, 225
 - clear_https_ta_cache, 227
 - element_name, 227
 - elements, 227
 - endElement, 225
 - serve_fetch_all, 226
 - serve_fetch_one_maybe, 226
 - serve_post_save_hook, 226
 - sql_template, 228
- rpki::publication::cms_msg, 228
 - encoding, 229

- saxify, 229
- schema, 229
- rpki::publication::config_elt, 229
 - attributes, 231
 - config_id, 231
 - element_name, 231
 - elements, 231
 - fetch, 230
 - serve_fetch_one_maybe, 230
 - serve_set, 230
 - sql_template, 232
 - startElement, 231
 - wired_in_config_id, 232
- rpki::publication::control_elt, 232
 - serve_dispatch, 233
- rpki::publication::crl_elt, 233
 - element_name, 233
 - payload_type, 233
- rpki::publication::manifest_elt, 234
 - element_name, 234
 - payload_type, 234
- rpki::publication::msg, 235
 - pdus, 236
 - serve_top_level, 235
 - version, 236
- rpki::publication::publication_
namespace, 236
 - nsmap, 237
 - xmlns, 237
- rpki::publication::publication_object_elt,
237
 - attributes, 240
 - endElement, 238
 - make_publish, 238
 - make_withdraw, 238
 - payload, 240
 - payload_type, 240
 - serve_dispatch, 238
 - serve_publish, 239
 - serve_withdraw, 239
 - toXML, 239
 - uri_to_filename, 239
- rpki::publication::report_error_elt, 240
 - __str__, 241
 - attributes, 242
 - element_name, 242
 - error_code, 242
 - error_text, 242
 - from_exception, 241
 - tag, 242
 - text_attribute, 242
- rpki::publication::roa_elt, 243
 - element_name, 243
 - payload_type, 243
- rpki::publication::sax_handler, 244
 - name, 244
 - pdu, 244
 - version, 244
- rpki::relaxng
 - left_right, 81
 - publication, 81
 - up_down, 81
- rpki::resource_set
 - _bs2long, 83
 - _long2bs, 83
 - _rsplit, 83
 - inherit_token, 84
 - test1, 83
 - test2, 84
- rpki::resource_set::resource_bag, 245
 - __eq__, 246
 - __init__, 246
 - __ne__, 246
 - __str__, 246
 - asn, 247
 - empty, 246
 - from_rfc3779_tuples, 246
 - intersection, 246
 - oversized, 247
 - undersized, 247
 - union, 247
 - v4, 247
 - v6, 248
 - valid_until, 248
- rpki::resource_set::resource_range, 248
 - __cmp__, 249
 - __init__, 249
 - max, 249
 - min, 249
- rpki::resource_set::resource_range_as,
250
 - __str__, 250

- datum_type, 251
- min, 251
- to_rfc3779_tuple, 250
- rpki::resource_set::resource_range_ip, 251
 - __str__, 252
 - _prefixlen, 252
 - make_prefix, 252
 - to_rfc3779_tuple, 252
- rpki::resource_set::resource_range_ipv4, 253
 - datum_type, 253
- rpki::resource_set::resource_range_ipv6, 254
 - datum_type, 254
- rpki::resource_set::resource_set, 254
 - __init__, 255
 - __str__, 255
 - _comm, 255
 - contains, 256
 - difference, 256
 - from_sql, 256
 - inherit, 258
 - intersection, 256
 - issubset, 257
 - issuperset, 257
 - symmetric_difference, 257
 - union, 257
- rpki::resource_set::resource_set_as, 258
 - inherit, 259
 - parse_rfc3779_tuple, 259
 - parse_str, 259
 - range_type, 259
 - to_rfc3779_tuple, 259
- rpki::resource_set::resource_set_ip, 260
 - inherit, 261
 - parse_rfc3779_tuple, 260
 - parse_str, 260
 - to_rfc3779_tuple, 261
- rpki::resource_set::resource_set_ipv4, 261
 - afi, 262
 - range_type, 262
- rpki::resource_set::resource_set_ipv6, 262
 - afi, 263
 - range_type, 263
- rpki::resource_set::roa_prefix, 263
 - __cmp__, 264
 - __init__, 264
 - __str__, 264
 - max, 265
 - max_prefixlen, 266
 - min, 265
 - prefix, 266
 - prefixlen, 266
 - to_resource_range, 265
 - to_roa_tuple, 265
- rpki::resource_set::roa_prefix_ipv4, 266
 - range_type, 267
- rpki::resource_set::roa_prefix_ipv6, 267
 - range_type, 267
- rpki::resource_set::roa_prefix_set, 268
 - __init__, 268
 - __str__, 268
 - from_sql, 268
 - parse_str, 269
 - to_resource_set, 269
 - to_roa_tuple, 269
- rpki::resource_set::roa_prefix_set_ipv4, 270
 - prefix_type, 270
 - resource_set_type, 270
- rpki::resource_set::roa_prefix_set_ipv6, 271
 - prefix_type, 271
 - resource_set_type, 271
- rpki::roa::ROAIPAddress, 272
 - __init__, 272
 - address, 272
 - maxLength, 272
- rpki::roa::ROAIPAddresses, 273
 - __init__, 273
- rpki::roa::ROAIPAddressFamilies, 273
 - __init__, 274
- rpki::roa::ROAIPAddressFamily, 274
 - __init__, 274
 - addresses, 275
 - addressFamily, 275
- rpki::roa::RouteOriginAttestation, 275
 - __init__, 275
 - asID, 276

- explicitVersion, 276
- ipAddrBlocks, 276
- version, 276
- rpki::rpki_engine::ca_detail_obj, 276
 - activate, 278
 - ca, 278
 - ca_cert_uri, 282
 - ca_id, 282
 - child_certs, 278
 - create, 278
 - crl_uri, 278
 - crl_uri_tail, 278
 - delete, 279
 - gctx, 282
 - generate_crl, 279
 - generate_manifest, 279
 - generate_manifest_cert, 279
 - issue, 280
 - issue_ee, 280
 - latest_ca_cert, 282
 - latest_crl, 282
 - latest_manifest, 282
 - latest_manifest_cert, 283
 - manifest_private_key_id, 283
 - manifest_public_key, 283
 - manifest_uri, 280
 - nextUpdate, 283
 - private_key_id, 283
 - public_key, 283
 - revoke, 280
 - revoked_certs, 281
 - roas, 281
 - sql_decode, 281
 - sql_template, 283
 - state, 284
 - update, 281
- rpki::rpki_engine::ca_obj, 284
 - ca_details, 285
 - check_for_updates, 285
 - construct_sia_uri, 286
 - create, 286
 - delete, 286
 - fetch_active, 286
 - fetch_deprecated, 287
 - fetch_nonnull_nonrevoked, 287
 - fetch_pending, 287
 - fetch_revoked, 287
 - gctx, 289
 - last_crl_sn, 289
 - last_issued_sn, 289
 - last_manifest_sn, 289
 - next_crl_number, 287
 - next_manifest_number, 288
 - next_serial_number, 288
 - parent, 288
 - parent_id, 289
 - parent_resource_class, 289
 - rekey, 288
 - revoke, 288
 - sia_uri, 290
 - sql_template, 290
- rpki::rpki_engine::child_cert_obj, 290
 - __init__, 291
 - ca_detail, 291
 - ca_detail_id, 293
 - cert, 293
 - child, 291
 - child_id, 293
 - fetch, 291
 - gctx, 293
 - reissue, 292
 - revoke, 292
 - sql_template, 293
 - uri, 292
 - uri_tail, 292
- rpki::rpki_engine::revoked_cert_obj, 294
 - __init__, 295
 - ca_detail, 295
 - ca_detail_id, 295
 - expires, 295
 - gctx, 295
 - revoke, 295
 - revoked, 296
 - serial, 296
 - sql_template, 296
- rpki::rpki_engine::roa_obj, 296
 - __init__, 297
 - asn, 300
 - ca_detail, 297
 - ca_detail_id, 300
 - cert, 300
 - gctx, 300

- generate, 298
- ipv4, 301
- ipv6, 301
- regenerate, 298
- revoke, 298
- roa, 301
- self, 299
- self_id, 301
- sql_delete_hook, 299
- sql_fetch_hook, 299
- sql_insert_hook, 299
- sql_template, 301
- update, 299
- uri, 300
- uri_tail, 300
- rpki::rpki_engine::rpkid_context, 302
 - __init__, 303
 - bpki_ta, 305
 - build_https_ta_cache, 303
 - clear_https_ta_cache, 303
 - cron, 303
 - cron_keepalive, 305
 - cron_period, 305
 - cron_timeout, 305
 - cronjob_handler, 304
 - https_server_host, 306
 - https_server_port, 306
 - https_ta_cache, 306
 - initial_delay, 306
 - irbe_cert, 306
 - irdb_cert, 306
 - irdb_query, 304
 - irdb_query_child_resources, 304
 - irdb_query_roa_requests, 304
 - irdb_url, 306
 - left_right_handler, 304
 - publication_kludge_base, 307
 - rpkid_cert, 307
 - rpkid_key, 307
 - sql, 307
 - start_cron, 305
 - up_down_handler, 305
 - up_down_url_regexp, 307
 - use_internal_cron, 307
- rpki::sql::session, 308
 - __init__, 309
 - _exceptions_enabled, 311
 - _wrap_execute, 309
 - assert_pristine, 309
 - cache, 311
 - cache_clear, 309
 - close, 309
 - connect, 309
 - cur, 311
 - database, 311
 - db, 311
 - dirty, 311
 - execute, 310
 - executemany, 310
 - fetchall, 310
 - lastrowid, 310
 - password, 311
 - ping, 310
 - sweep, 310
 - username, 311
- rpki::sql::sql_persistent, 312
 - gctx, 317
 - sql_debug, 317
 - sql_decode, 313
 - sql_delete, 313
 - sql_delete_hook, 313
 - sql_deleted, 317
 - sql_encode, 314
 - sql_fetch, 314
 - sql_fetch_all, 314
 - sql_fetch_hook, 314
 - sql_fetch_where, 315
 - sql_fetch_where1, 315
 - sql_in_db, 317
 - sql_init, 315
 - sql_insert_hook, 315
 - sql_is_dirty, 315
 - sql_mark_clean, 316
 - sql_mark_deleted, 316
 - sql_mark_dirty, 316
 - sql_store, 316
 - sql_update_hook, 316
- rpki::sql::template, 318
 - __init__, 318
 - columns, 318
 - delete, 318
 - index, 319

- insert, 319
- map, 319
- select, 319
- table, 319
- update, 319
- rpki::sundial
 - _cast, 88
 - now, 88
 - test, 88
- rpki::sundial::datetime, 320
 - __add__, 321
 - __radd__, 321
 - __rsub__, 321
 - __str__, 321
 - __sub__, 321
 - earlier, 321
 - from_sql, 321
 - fromASN1tuple, 322
 - fromdatetime, 322
 - fromGeneralizedTime, 322
 - fromUTCtime, 322
 - fromXMLtime, 322
 - later, 322
 - PKIX_threshold, 324
 - to_sql, 323
 - toASN1tuple, 323
 - toGeneralizedTime, 323
 - totimestamp, 323
 - toUTCtime, 323
 - toXMLtime, 324
- rpki::sundial::timedelta, 324
 - __abs__, 325
 - __add__, 325
 - __div__, 325
 - __floordiv__, 326
 - __mul__, 326
 - __neg__, 326
 - __pos__, 326
 - __radd__, 326
 - __rdiv__, 326
 - __rfloordiv__, 326
 - __rmul__, 327
 - __rsub__, 327
 - __sub__, 327
 - convert_to_seconds, 327
 - fromtimedelta, 327
 - parse, 327
 - regexp, 328
- rpki::up_down
 - nsmmap, 90
 - xmlns, 90
- rpki::up_down::base_elt, 328
 - check_response, 329
 - endElement, 329
 - make_b64elt, 329
 - make_elt, 329
 - serve_pdu, 330
 - startElement, 330
- rpki::up_down::certificate_elt, 330
 - cert, 332
 - cert_url, 332
 - endElement, 331
 - req_resource_set_as, 332
 - req_resource_set_ipv4, 332
 - req_resource_set_ipv6, 332
 - startElement, 331
 - toXML, 331
- rpki::up_down::class_elt, 333
 - __init__, 333
 - cert_url, 335
 - certs, 335
 - class_name, 335
 - endElement, 333
 - from_resource_bag, 334
 - issuer, 335
 - resource_set_as, 335
 - resource_set_ipv4, 335
 - resource_set_ipv6, 335
 - resource_set_notafter, 335
 - startElement, 334
 - suggested_sia_head, 336
 - to_resource_bag, 334
 - toXML, 334
- rpki::up_down::class_response_syntax, 336
 - __init__, 336
 - classes, 337
 - startElement, 337
 - toXML, 337
- rpki::up_down::cms_msg, 337
 - encoding, 338
 - saxify, 338

- schema, 338
- rpki::up_down::error_response_pdu, 338
 - __init__, 339
 - check_response, 339
 - codes, 340
 - description, 340
 - endElement, 339
 - exceptions, 340
 - status, 341
 - toXML, 340
- rpki::up_down::issue_pdu, 341
 - class_name, 343
 - endElement, 342
 - pkcs10, 343
 - query, 342
 - req_resource_set_as, 343
 - req_resource_set_ipv4, 343
 - req_resource_set_ipv6, 343
 - serve_pdu, 342
 - startElement, 342
 - toXML, 343
- rpki::up_down::issue_response_pdu, 344
 - check_response, 344
- rpki::up_down::list_pdu, 344
 - query, 345
 - serve_pdu, 345
 - toXML, 345
- rpki::up_down::list_response_pdu, 346
- rpki::up_down::message_pdu, 346
 - __str__, 347
 - log_query, 347
 - make_query, 347
 - name2type, 348
 - payload, 349
 - recipient, 349
 - sender, 349
 - serve_error, 347
 - serve_top_level, 347
 - startElement, 348
 - toXML, 348
 - type, 349
 - type2name, 349
 - version, 349
- rpki::up_down::multi_uri, 350
 - __init__, 350
 - __str__, 350
- rsync, 350
- rpki::up_down::revoke_pdu, 351
 - class_name, 352
 - get_SKI, 351
 - query, 351
 - serve_pdu, 352
 - ski, 352
- rpki::up_down::revoke_response_pdu, 352
- rpki::up_down::revoke_syntax, 353
 - class_name, 354
 - ski, 354
 - startElement, 353
 - toXML, 353
- rpki::up_down::sax_handler, 354
 - name, 355
 - pdu, 355
 - version, 355
- rpki::x509
 - calculate_SKI, 92
 - POWify_OID, 92
- rpki::x509::CMS_object, 355
 - content, 358
 - debug_cms_certs, 358
 - DER, 358
 - dump_on_verify_failure, 359
 - econtent_oid, 359
 - extract, 357
 - formats, 359
 - get_content, 357
 - get_DER, 357
 - get_POW, 357
 - other_clear, 359
 - pem_converter, 359
 - POW, 360
 - print_on_der_error, 360
 - require_crls, 360
 - set_content, 357
 - sign, 358
 - verify, 358
- rpki::x509::CRL, 360
 - DER, 363
 - formats, 363
 - generate, 361
 - get_DER, 361
 - get_POW, 362

- get_POWpkix, 362
- getIssuer, 362
- getNextUpdate, 362
- getThisUpdate, 362
- pem_converter, 363
- POW, 363
- POWpkix, 363
- rpki::x509::DER_CMS_object, 364
 - content, 365
 - decode, 364
 - encode, 364
- rpki::x509::DER_object, 365
 - __cmp__, 366
 - __init__, 366
 - clear, 367
 - DER, 371
 - dumpasn1, 367
 - empty, 367
 - formats, 371
 - from_sql, 367
 - gAKI, 367
 - get_3779resources, 368
 - get_AIA, 368
 - get_AKI, 368
 - get_Base64, 368
 - get_basicConstraints, 368
 - get_DER, 369
 - get_PEM, 369
 - get_SIA, 369
 - get_SKI, 369
 - gSKI, 370
 - hAKI, 370
 - hSKI, 370
 - is_CA, 370
 - other_clear, 371
 - pem_converter, 372
 - set, 370
 - to_sql, 371
- rpki::x509::PEM_converter, 372
 - __init__, 373
 - b, 373
 - e, 373
 - looks_like_PEM, 373
 - to_DER, 373
 - to_PEM, 373
- rpki::x509::PKCS10, 374
 - check_valid_rpki, 375
 - create, 375
 - create_ca, 375
 - DER, 376
 - formats, 376
 - get_DER, 375
 - get_POWpkix, 375
 - getPublicKey, 376
 - pem_converter, 376
 - POWpkix, 377
- rpki::x509::ROA, 377
 - build, 377
 - content_class, 378
 - econtent_oid, 378
 - pem_converter, 378
- rpki::x509::RSA, 378
 - DER, 380
 - formats, 380
 - generate, 379
 - get_DER, 379
 - get_POW, 379
 - get_public_DER, 380
 - get_RSAPublic, 380
 - get_SKI, 380
 - pem_converter, 381
 - POW, 381
- rpki::x509::RSAPublic, 381
 - DER, 383
 - formats, 383
 - get_DER, 382
 - get_POW, 382
 - get_SKI, 382
 - pem_converter, 383
 - POW, 383
- rpki::x509::SignedManifest, 383
 - build, 384
 - content_class, 385
 - econtent_oid, 385
 - getNextUpdate, 384
 - getThisUpdate, 384
 - pem_converter, 385
- rpki::x509::X509, 385
 - cross_certify, 387
 - DER, 389
 - expired, 387
 - formats, 389

- get_DER, 387
- get_POW, 387
- get_POWpkix, 387
- getIssuer, 387
- getNotAfter, 388
- getNotBefore, 388
- getPublicKey, 388
- getSerial, 388
- getSubject, 388
- issue, 389
- normalize_chain, 389
- pem_converter, 390
- POW, 390
- POWpkix, 390
- rpki::x509::XML_CMS_object, 390
 - content, 393
 - decode, 391
 - dump_inbound_cms, 393
 - dump_outbound_cms, 393
 - dump_to_disk, 391
 - content_oid, 393
 - encode, 391
 - pretty_print_content, 392
 - schema_check, 392
 - unwrap, 392
 - wrap, 392
- rpki::xml_utils::base_elt, 393
 - __str__, 394
 - attributes, 396
 - booleans, 396
 - elements, 397
 - endElement, 395
 - make_b64elt, 395
 - make_elt, 395
 - make_pdu, 395
 - read_attrs, 395
 - startElement, 396
 - toXML, 396
- rpki::xml_utils::data_elt, 397
 - endElement, 398
 - make_reply, 398
 - make_reply_clone_hook, 398
 - serve_create, 398
 - serve_destroy, 399
 - serve_destroy_hook, 399
 - serve_dispatch, 399
 - serve_fetch_one, 399
 - serve_get, 399
 - serve_list, 400
 - serve_post_save_hook, 400
 - serve_pre_save_hook, 400
 - serve_set, 400
 - toXML, 401
 - unimplemented_control, 401
- rpki::xml_utils::msg, 401
 - __str__, 402
 - endElement, 402
 - is_query, 402
 - is_reply, 402
 - query, 402
 - reply, 403
 - startElement, 403
 - toXML, 403
 - type, 403
 - version, 403
- rpki::xml_utils::sax_handler, 404
 - __init__, 405
 - characters, 405
 - create_top_level, 405
 - endElement, 405
 - endElementNS, 405
 - result, 407
 - saxify, 406
 - stack, 407
 - startElement, 406
 - startElementNS, 406
 - text, 407
- rpki::xml_utils::text_elt, 407
 - endElement, 408
 - text_attribute, 408
 - toXML, 408
- rpki_base_uri
 - rootd, 60
- rpki_class_name
 - rootd, 61
- rpki_content_type
 - rpki::https, 71
- rpki_engine.py(2793), 422
- rpki_root_cert
 - rootd, 61
- rpki_root_cert_file
 - rootd, 61

- rpki_root_cert_uri
 - rootd, [61](#)
- rpki_root_crl
 - rootd, [61](#)
- rpki_root_dir
 - rootd, [61](#)
- rpki_root_key
 - rootd, [61](#)
- rpki_root_manifest
 - rootd, [62](#)
- rpki_subject_cert
 - rootd, [62](#)
- rpki_subject_lifetime
 - rootd, [62](#)
- rpki_subject_pkcs10
 - rootd, [62](#)
- rpki_subject_regen
 - rootd, [62](#)
- rpkid, [93](#)
 - cfg_file, [94](#)
 - main, [94](#)
 - profile, [94](#)
- rpkid.py(2799), [422](#)
- rpkid_cert
 - irbdb, [53](#)
 - rpki::rpki_engine::rpkid_context, [307](#)
- rpkid_key
 - rpki::rpki_engine::rpkid_context, [307](#)
- rsync
 - rpki::up_down::multi_uri, [350](#)
- runq
 - rpki::async::timer, [129](#)
- saxify
 - irbe_cli::left_right_cms_msg, [106](#)
 - irbe_cli::publication_cms_msg, [109](#)
 - rootd::cms_msg, [118](#)
 - rpki::left_right::cms_msg, [188](#)
 - rpki::publication::cms_msg, [229](#)
 - rpki::up_down::cms_msg, [338](#)
 - rpki::xml_utils::sax_handler, [406](#)
- schema
 - rpki::left_right::cms_msg, [188](#)
 - rpki::publication::cms_msg, [229](#)
 - rpki::up_down::cms_msg, [338](#)
- schema_check
 - rpki::x509::XML_CMS_object, [392](#)
- seconds_until_wakeup
 - rpki::async::timer, [129](#)
- select
 - rpki::sql::template, [319](#)
- self
 - rpki::left_right::data_elt, [190](#)
 - rpki::rpki_engine::roa_obj, [299](#)
- self_handle
 - rpki::left_right::data_elt, [191](#)
 - rpki::left_right::report_error_elt, [207](#)
- self_id
 - rpki::left_right::data_elt, [191](#)
 - rpki::rpki_engine::roa_obj, [301](#)
- send
 - rpki::https::http_stream, [174](#)
- send_error
 - rpki::https::http_server, [169](#)
- send_message
 - rpki::https::http_server, [169](#)
- send_reply
 - rpki::https::http_server, [169](#)
- send_request
 - rpki::https::http_client, [154](#)
 - rpki::https::http_queue, [163](#)
- sender
 - rpki::up_down::message_pdu, [349](#)
- Sequence, [409](#)
- SequenceOf, [409](#)
- serial
 - rpki::rpki_engine::revoked_cert_obj, [296](#)
- serve_create
 - rpki::xml_utils::data_elt, [398](#)
- serve_destroy
 - rpki::xml_utils::data_elt, [399](#)
- serve_destroy_hook
 - rpki::left_right::child_elt, [185](#)
 - rpki::xml_utils::data_elt, [399](#)
- serve_dispatch
 - rpki::left_right::list_published_objects_elt, [193](#)
 - rpki::publication::control_elt, [233](#)

- rpki::publication::publication_
 object_elt, 238
- rpki::xml_utils::data_elt, 399
- serve_error
 - rpki::up_down::message_pdu, 347
- serve_fetch_all
 - rpki::left_right::data_elt, 190
 - rpki::left_right::self_elt, 214
 - rpki::publication::client_elt, 226
- serve_fetch_handle
 - rpki::left_right::data_elt, 190
 - rpki::left_right::self_elt, 215
- serve_fetch_one
 - rpki::xml_utils::data_elt, 399
- serve_fetch_one_maybe
 - rpki::left_right::data_elt, 190
 - rpki::left_right::self_elt, 215
 - rpki::publication::client_elt, 226
 - rpki::publication::config_elt, 230
- serve_get
 - rpki::xml_utils::data_elt, 399
- serve_list
 - rpki::xml_utils::data_elt, 400
- serve_pdu
 - rootd::issue_pdu, 119
 - rootd::list_pdu, 120
 - rootd::revoke_pdu, 122
 - rpki::up_down::base_elt, 330
 - rpki::up_down::issue_pdu, 342
 - rpki::up_down::list_pdu, 345
 - rpki::up_down::revoke_pdu, 352
- serve_post_save_hook
 - rpki::left_right::child_elt, 185
 - rpki::left_right::parent_elt, 202
 - rpki::left_right::self_elt, 215
 - rpki::publication::client_elt, 226
 - rpki::xml_utils::data_elt, 400
- serve_pre_save_hook
 - rpki::left_right::bsc_elt, 181
 - rpki::left_right::data_elt, 191
 - rpki::xml_utils::data_elt, 400
- serve_publish
 - rpki::publication::publication_
 object_elt, 239
- serve_publish_world_now
 - rpki::left_right::self_elt, 215
- serve_rekey
 - rpki::left_right::parent_elt, 202
 - rpki::left_right::self_elt, 216
- serve_revoke
 - rpki::left_right::parent_elt, 202
 - rpki::left_right::self_elt, 216
- serve_revoke_forgotten
 - rpki::left_right::parent_elt, 202
 - rpki::left_right::self_elt, 216
- serve_run_now
 - rpki::left_right::self_elt, 216
- serve_set
 - rpki::publication::config_elt, 230
 - rpki::xml_utils::data_elt, 400
- serve_top_level
 - rpki::left_right::msg, 199
 - rpki::publication::msg, 235
 - rpki::up_down::message_pdu, 347
- serve_up_down
 - rpki::left_right::child_elt, 186
- serve_withdraw
 - rpki::publication::publication_
 object_elt, 239
- server
 - rpki::https, 70
- server_cert
 - irbe_cli::caller, 98
 - irdbd, 53
 - rootd, 62
- server_ta
 - irbe_cli::caller, 98
- set
 - rpki::async::timer, 130
 - rpki::x509::DER_object, 370
- set_content
 - rpki::x509::CMS_object, 357
- set_errback
 - rpki::async::timer, 130
- set_handler
 - rpki::async::timer, 130
- set_state
 - rpki::https::http_client, 154
- set_subject_cert
 - rootd, 58
- set_subject_pkcs10
 - rootd, 58

- set_trace
 - rpki::log, 75
- sia_uri
 - rpki::rpki_engine::ca_obj, 290
- sign
 - rpki::x509::CMS_object, 358
- signing_cert
 - irbe_cli::bsc_elt, 96
 - rpki::left_right::bsc_elt, 182
- signing_cert_crl
 - irbe_cli::bsc_elt, 96
 - rpki::left_right::bsc_elt, 183
- ski
 - rpki::up_down::revoke_pdu, 352
 - rpki::up_down::revoke_syntax, 354
- software_name
 - rpki::https::http_message, 161
- sql
 - pubd::pubd_context, 117
 - rpki::rpki_engine::rpkid_context, 307
- sql.py(2648), 422
- sql_debug
 - rpki::sql::sql_persistent, 317
- sql_decode
 - rpki::rpki_engine::ca_detail_obj, 281
 - rpki::sql::sql_persistent, 313
- sql_delete
 - rpki::sql::sql_persistent, 313
- sql_delete_hook
 - rpki::rpki_engine::roa_obj, 299
 - rpki::sql::sql_persistent, 313
- sql_deleted
 - rpki::sql::sql_persistent, 317
- sql_encode
 - rpki::sql::sql_persistent, 314
- sql_fetch
 - rpki::sql::sql_persistent, 314
- sql_fetch_all
 - rpki::sql::sql_persistent, 314
- sql_fetch_hook
 - rpki::rpki_engine::roa_obj, 299
 - rpki::sql::sql_persistent, 314
- sql_fetch_where
 - rpki::sql::sql_persistent, 315
- sql_fetch_where1
 - rpki::sql::sql_persistent, 315
- sql_in_db
 - rpki::sql::sql_persistent, 317
- sql_init
 - rpki::sql::sql_persistent, 315
- sql_insert_hook
 - rpki::rpki_engine::roa_obj, 299
 - rpki::sql::sql_persistent, 315
- sql_is_dirty
 - rpki::sql::sql_persistent, 315
- sql_mark_clean
 - rpki::sql::sql_persistent, 316
- sql_mark_deleted
 - rpki::sql::sql_persistent, 316
- sql_mark_dirty
 - rpki::sql::sql_persistent, 316
- sql_store
 - rpki::sql::sql_persistent, 316
- sql_template
 - rpki::left_right::bsc_elt, 183
 - rpki::left_right::child_elt, 187
 - rpki::left_right::parent_elt, 205
 - rpki::left_right::repository_elt, 210
 - rpki::left_right::self_elt, 219
 - rpki::publication::client_elt, 228
 - rpki::publication::config_elt, 232
 - rpki::rpki_engine::ca_detail_obj, 283
 - rpki::rpki_engine::ca_obj, 290
 - rpki::rpki_engine::child_cert_obj, 293
 - rpki::rpki_engine::revoked_cert_obj, 296
 - rpki::rpki_engine::roa_obj, 301
- sql_update_hook
 - rpki::sql::sql_persistent, 316
- stack
 - rpki::xml_utils::sax_handler, 407
- start
 - rpki::https::http_client, 155
- start_cron
 - rpki::rpki_engine::rpkid_context, 305
- startElement

- rpki::left_right::list_resources_elt, 195
- rpki::left_right::list_roa_requests_elt, 198
- rpki::publication::config_elt, 231
- rpki::up_down::base_elt, 330
- rpki::up_down::certificate_elt, 331
- rpki::up_down::class_elt, 334
- rpki::up_down::class_response_syntax, 337
- rpki::up_down::issue_pdu, 342
- rpki::up_down::message_pdu, 348
- rpki::up_down::revoke_syntax, 353
- rpki::xml_utils::base_elt, 396
- rpki::xml_utils::msg, 403
- rpki::xml_utils::sax_handler, 406
- startElementNS
 - rpki::xml_utils::sax_handler, 406
- startup_msg
 - irdbd, 53
- state
 - rpki::https::http_client, 156
 - rpki::rpki_engine::ca_detail_obj, 284
- status
 - rpki::up_down::error_response_pdu, 341
- suggested_sia_head
 - rpki::up_down::class_elt, 336
- sundial.py(2785), 423
- sweep
 - rpki::sql::session, 310
- symmetric_difference
 - rpki::resource_set::resource_set, 257
- ta
 - rpki::https::http_client, 156
 - rpki::https::http_listener, 158
 - rpki::https::http_queue, 164
- table
 - rpki::sql::template, 319
- tag
 - rpki::left_right::report_error_elt, 207
 - rpki::log, 77
 - rpki::publication::report_error_elt, 242
- test
 - rpki::sundial, 88
- test1
 - rpki::resource_set, 83
- test2
 - rpki::resource_set, 84
- text
 - rpki::xml_utils::sax_handler, 407
- text_attribute
 - rpki::left_right::list_published_objects_elt, 194
 - rpki::left_right::report_error_elt, 207
 - rpki::publication::report_error_elt, 242
 - rpki::xml_utils::text_elt, 408
- textwrap::TextWrapper, 409
- thisUpdate
 - rpki::manifest::Manifest, 223
- timeout
 - rpki::https::http_client, 156
 - rpki::https::http_server, 170
- timer
 - rpki::async::iterator, 125
 - rpki::https::http_stream, 176
- tls
 - rpki::https::http_client, 156
 - rpki::https::http_server, 170
 - rpki::https::http_stream, 176
- tls_accept
 - rpki::https::http_server, 169
- tls_connect
 - rpki::https::http_client, 155
- to_bytes
 - rpki::ipaddr::v4addr, 177
 - rpki::ipaddr::v6addr, 179
- to_DER
 - rpki::x509::PEM_converter, 373
- to_PEM
 - rpki::x509::PEM_converter, 373
- to_resource_bag
 - rpki::up_down::class_elt, 334
- to_resource_range
 - rpki::resource_set::roa_prefix, 265
- to_resource_set
 - rpki::resource_set::roa_prefix_set, 269

- to_rfc3779_tuple
 - rpki::resource_set::resource_range_-as, 250
 - rpki::resource_set::resource_range_ip, 252
 - rpki::resource_set::resource_set_as, 259
 - rpki::resource_set::resource_set_ip, 261
- to_roa_tuple
 - rpki::resource_set::roa_prefix, 265
 - rpki::resource_set::roa_prefix_set, 269
- to_sql
 - rpki::sundial::datetime, 323
 - rpki::x509::DER_object, 371
- toASN1tuple
 - rpki::sundial::datetime, 323
- toGeneralizedTime
 - rpki::sundial::datetime, 323
- top_opts
 - irbe_cli, 48
- totimestamp
 - rpki::sundial::datetime, 323
- toUTCTime
 - rpki::sundial::datetime, 323
- toXML
 - rpki::left_right::list_resources_elt, 196
 - rpki::publication::publication_object_elt, 239
 - rpki::up_down::certificate_elt, 331
 - rpki::up_down::class_elt, 334
 - rpki::up_down::class_response_syntax, 337
 - rpki::up_down::error_response_pdu, 340
 - rpki::up_down::issue_pdu, 343
 - rpki::up_down::list_pdu, 345
 - rpki::up_down::message_pdu, 348
 - rpki::up_down::revoke_syntax, 353
 - rpki::xml_utils::base_elt, 396
 - rpki::xml_utils::data_elt, 401
 - rpki::xml_utils::msg, 403
 - rpki::xml_utils::text_elt, 408
- toXMLtime
 - rpki::sundial::datetime, 324
- trace
 - rpki::log, 75
- traceback
 - rpki::log, 75
- type
 - rpki::up_down::message_pdu, 349
 - rpki::xml_utils::msg, 403
- type2name
 - rootd::message_pdu, 121
 - rpki::up_down::message_pdu, 349
- u
 - irbdb, 53
- undersized
 - rpki::resource_set::resource_bag, 247
- unimplemented_control
 - rpki::xml_utils::data_elt, 401
- union
 - rpki::resource_set::resource_bag, 247
 - rpki::resource_set::resource_set, 257
- unwrap
 - rpki::x509::XML_CMS_object, 392
- up_down
 - rpki::relaxng, 81
- up_down.py(2793), 423
- up_down_handler
 - rootd, 58
 - rpki::rpki_engine::rpkid_context, 305
- up_down_url_regexp
 - rpki::rpki_engine::rpkid_context, 307
- update
 - rpki::rpki_engine::ca_detail_obj, 281
 - rpki::rpki_engine::roa_obj, 299
 - rpki::sql::template, 319
- update_children
 - rpki::left_right::self_elt, 217
- update_roas
 - rpki::left_right::self_elt, 217
- update_timeout
 - rpki::https::http_stream, 174

- uri
 - rpki::rpki_engine::child_cert_obj, 292
 - rpki::rpki_engine::roa_obj, 300
- uri_tail
 - rpki::rpki_engine::child_cert_obj, 292
 - rpki::rpki_engine::roa_obj, 300
- uri_to_filename
 - rpki::publication::publication_object_elt, 239
- url
 - irbe_cli::caller, 98
- usage
 - irbe_cli, 46
 - irbe_cli::cmd_elt_mixin, 102
 - irbe_cli::cmd_msg_mixin, 104
- usage_fill
 - irbe_cli, 48
- use_hsm
 - rpki::left_right::self_elt, 219
- use_internal_cron
 - rpki::rpki_engine::rpkiid_context, 307
- use_syslog
 - rpki::log, 77
- username
 - rpki::sql::session, 311
- v4
 - rpki::resource_set::resource_bag, 247
- v6
 - rpki::resource_set::resource_bag, 248
- valid_until
 - rpki::left_right::list_resources_elt, 197
 - rpki::resource_set::resource_bag, 248
- verbose
 - irbe_cli, 49
- verify
 - rpki::x509::CMS_object, 358
- version
 - rpki::https::http_message, 161
 - rpki::left_right::msg, 200
 - rpki::left_right::sax_handler, 211
 - rpki::manifest::Manifest, 223
 - rpki::publication::msg, 236
 - rpki::publication::sax_handler, 244
 - rpki::roa::RouteOriginAttestation, 276
 - rpki::up_down::message_pdu, 349
 - rpki::up_down::sax_handler, 355
 - rpki::xml_utils::msg, 403
- want_persistent_client
 - rpki::https, 71
- want_persistent_server
 - rpki::https, 71
- warn
 - rpki::log, 77
- when
 - rpki::async::timer, 131
- wired_in_config_id
 - rpki::publication::config_elt, 232
- withdraw
 - rpki::left_right::repository_elt, 209
- wrap
 - rpki::x509::XML_CMS_object, 392
- writable
 - rpki::https::http_stream, 175
- x509.py(2784), 424
- xml::sax::handler::ContentHandler, 409
- xml_utils.py(2791), 424
- xmlns
 - rpki::left_right::left_right_namespace, 192
 - rpki::publication::publication_namespace, 237
 - rpki::up_down, 90