

RPKI Engine

1.0

Generated by Doxygen 1.5.8

Mon Jun 8 18:22:48 2009

Contents

1	RPKI Engine Reference Manual	1
2	Further Reading	1
3	Installation Guide	2
4	Operation Guide	4
4.1	rpkid.py	6
4.2	pubd.py	7
4.3	rootd.py	8
4.4	irdbd.py	9
4.5	irbe_cli.py	10
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	18
5.2.1	<self/> object	19
5.2.2	<bsc/> object	21
5.2.3	<parent/> object	22
5.2.4	<child/> object	23
5.2.5	<repository/> object	24
5.2.6	<route_origin/> object	25
5.3	Operations initiated by the RPKI engine	26
5.3.1	<list_resources/> messages	26
5.4	Error handling	27
6	Publication protocol	28

6.1	Terminology	28
6.2	Publication control subprotocol	28
6.2.1	<config/> object	28
6.2.2	<client/> object	29
6.3	Publication subprotocol	29
6.3.1	<certificate/> object	30
6.3.2	<crl/> object	30
6.3.3	<manifest/> object	30
6.3.4	<roa/> object	30
6.4	Error handling	30
6.5	Additional access control considerations.	31
7	SQL database schemas	32
7.1	rpkid SQL schema	34
7.2	pubd SQL Schema	38
7.3	irdbd SQL Schema	40
8	BPKI model	42
9	Namespace Documentation	45
9.1	Package cross_certify	45
9.1.1	Detailed Description	45
9.1.2	Function Documentation	46
9.1.3	Variable Documentation	46
9.2	Package irbe_cli	48
9.2.1	Detailed Description	50
9.2.2	Function Documentation	50
9.2.3	Variable Documentation	51
9.3	Package irdbd	53
9.3.1	Detailed Description	53
9.3.2	Function Documentation	54
9.3.3	Variable Documentation	54

9.4	Package pubd	57
9.4.1	Detailed Description	57
9.4.2	Function Documentation	58
9.4.3	Variable Documentation	58
9.5	Package rootd	58
9.5.1	Detailed Description	60
9.5.2	Function Documentation	60
9.5.3	Variable Documentation	61
9.6	Package rpki	65
9.7	Package rpki.async	66
9.7.1	Detailed Description	66
9.7.2	Function Documentation	67
9.7.3	Variable Documentation	67
9.8	Package rpki.config	67
9.8.1	Detailed Description	68
9.9	Package rpki.exceptions	68
9.9.1	Detailed Description	69
9.10	Package rpki.https	70
9.10.1	Detailed Description	71
9.10.2	Function Documentation	71
9.10.3	Variable Documentation	72
9.11	Package rpki.ipaddrs	73
9.11.1	Detailed Description	74
9.12	Package rpki.left_right	74
9.12.1	Detailed Description	75
9.12.2	Variable Documentation	76
9.13	Package rpki.log	76
9.13.1	Detailed Description	76
9.13.2	Function Documentation	77
9.13.3	Variable Documentation	78
9.14	Package rpki.manifest	79

9.14.1 Detailed Description	79
9.15 Package rpki.oids	80
9.15.1 Detailed Description	80
9.15.2 Variable Documentation	80
9.16 Package rpki.publication	81
9.16.1 Detailed Description	82
9.16.2 Variable Documentation	83
9.17 Package rpki.relaxng	83
9.17.1 Variable Documentation	83
9.18 Package rpki.resource_set	84
9.18.1 Detailed Description	85
9.18.2 Function Documentation	85
9.18.3 Variable Documentation	86
9.19 Package rpki.roa	86
9.19.1 Detailed Description	87
9.20 Package rpki.rpki_engine	88
9.20.1 Detailed Description	88
9.21 Package rpki.sql	88
9.21.1 Detailed Description	89
9.22 Package rpki.sundial	89
9.22.1 Detailed Description	89
9.22.2 Function Documentation	90
9.23 Package rpki.up_down	91
9.23.1 Detailed Description	91
9.23.2 Variable Documentation	92
9.24 Package rpki.x509	92
9.24.1 Detailed Description	93
9.24.2 Function Documentation	94
9.25 Package rpki.xml_utils	94
9.25.1 Detailed Description	94
9.26 Package rpkid	95

9.26.1 Detailed Description	95
9.26.2 Function Documentation	96
9.26.3 Variable Documentation	96
10 Class Documentation	96
10.1 asynchat.async_chat Class Reference	96
10.2 asyncore.dispatcher Class Reference	97
10.3 ConfigParser.RawConfigParser Class Reference	97
10.4 Exception Class Reference	97
10.5 irbe_cli.bsc_elt Class Reference	97
10.5.1 Detailed Description	98
10.5.2 Member Function Documentation	98
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	100
10.8.1 Detailed Description	100
10.9 irbe_cli.cmd_elt_mixin Class Reference	100
10.9.1 Detailed Description	101
10.9.2 Member Function Documentation	101
10.9.3 Member Data Documentation	103
10.10 irbe_cli.cmd_msg_mixin Class Reference	104
10.10.1 Detailed Description	104
10.10.2 Member Function Documentation	104
10.11 irbe_cli.config_elt Class Reference	105
10.11.1 Detailed Description	105
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	106
10.13irbe_cli.left_right_cms_msg Class Reference	106
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	107
10.14.2 Member Data Documentation	107
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.manifest_elt Class Reference	108
10.16.1 Detailed Description	108
10.17irbe_cli.parent_elt Class Reference	108
10.17.1 Detailed Description	108
10.18irbe_cli.publication_cms_msg Class Reference	108
10.18.1 Detailed Description	108
10.18.2 Member Data Documentation	109
10.19irbe_cli.publication_msg Class Reference	109
10.19.1 Detailed Description	109
10.19.2 Member Data Documentation	109
10.20irbe_cli.publication_sax_handler Class Reference	110
10.20.1 Detailed Description	110
10.20.2 Member Data Documentation	110
10.21irbe_cli.repository_elt Class Reference	110
10.21.1 Detailed Description	110
10.22irbe_cli.roa_elt Class Reference	110
10.22.1 Detailed Description	111
10.23irbe_cli.route_origin_elt Class Reference	111
10.23.1 Detailed Description	111
10.23.2 Member Function Documentation	111
10.23.3 Member Data Documentation	112

10.24	irbe_cli.self_elt Class Reference	113
10.24.1	Detailed Description	113
10.25	irbe_cli.UsageWrapper Class Reference	113
10.25.1	Detailed Description	113
10.25.2	Member Function Documentation	113
10.26	long Class Reference	114
10.27	object Class Reference	114
10.28	pubd.pubd_context Class Reference	114
10.28.1	Detailed Description	115
10.28.2	Member Function Documentation	115
10.28.3	Member Data Documentation	116
10.29	pydatetime.datetime Class Reference	118
10.30	pydatetime.timedelta Class Reference	118
10.31	rootd.cms_msg Class Reference	118
10.31.1	Detailed Description	118
10.31.2	Member Data Documentation	118
10.32	rootd.issue_pdu Class Reference	119
10.32.1	Detailed Description	119
10.32.2	Member Function Documentation	119
10.33	rootd.list_pdu Class Reference	119
10.33.1	Detailed Description	119
10.33.2	Member Function Documentation	120
10.34	rootd.message_pdu Class Reference	120
10.34.1	Detailed Description	120
10.34.2	Member Data Documentation	120
10.35	rootd.revoke_pdu Class Reference	121
10.35.1	Detailed Description	121
10.35.2	Member Function Documentation	121
10.36	rootd.sax_handler Class Reference	122
10.36.1	Detailed Description	122
10.36.2	Member Data Documentation	122

10.37rpki.async.iterator Class Reference	122
10.37.1 Detailed Description	123
10.37.2 Member Function Documentation	123
10.37.3 Member Data Documentation	124
10.38rpki.async.timer Class Reference	124
10.38.1 Detailed Description	125
10.38.2 Member Function Documentation	125
10.38.3 Member Data Documentation	128
10.39rpki.config.parser Class Reference	129
10.39.1 Detailed Description	129
10.39.2 Member Function Documentation	129
10.39.3 Member Data Documentation	130
10.40rpki.exceptions.BadClassNameSyntax Class Reference	130
10.40.1 Detailed Description	130
10.41rpki.exceptions.BadClientURL Class Reference	131
10.41.1 Detailed Description	131
10.42rpki.exceptions.BadContactURL Class Reference	131
10.42.1 Detailed Description	131
10.43rpki.exceptions.BadExtension Class Reference	131
10.43.1 Detailed Description	131
10.44rpki.exceptions.BadIRDBReply Class Reference	132
10.44.1 Detailed Description	132
10.45rpki.exceptions.BadIssueResponse Class Reference	132
10.45.1 Detailed Description	132
10.46rpki.exceptions.BadPKCS10 Class Reference	132
10.46.1 Detailed Description	132
10.47rpki.exceptions.BadPublicationReply Class Reference	133
10.47.1 Detailed Description	133
10.48rpki.exceptions.BadQuery Class Reference	133
10.48.1 Detailed Description	133
10.49rpki.exceptions.BadSender Class Reference	133

10.49.1 Detailed Description	133
10.50rpki.exceptions.BadStatusCode Class Reference	134
10.50.1 Detailed Description	134
10.51rpki.exceptions.BadURISyntax Class Reference	134
10.51.1 Detailed Description	134
10.52rpki.exceptions.BSCNotFound Class Reference	134
10.52.1 Detailed Description	134
10.53rpki.exceptions.ChildNotFound Class Reference	135
10.53.1 Detailed Description	135
10.54rpki.exceptions.ClassNameMismatch Class Reference	135
10.54.1 Detailed Description	135
10.55rpki.exceptions.ClassNameUnknown Class Reference	135
10.55.1 Detailed Description	135
10.56rpki.exceptions.ClientNotFound Class Reference	136
10.56.1 Detailed Description	136
10.57rpki.exceptions.CMSCRLNotSet Class Reference	136
10.57.1 Detailed Description	136
10.58rpki.exceptions.CMSVerificationFailed Class Reference	136
10.58.1 Detailed Description	136
10.59rpki.exceptions.DBConsistencyError Class Reference	137
10.59.1 Detailed Description	137
10.60rpki.exceptions.DERObjectConversionError Class Reference	137
10.60.1 Detailed Description	137
10.61rpki.exceptions.DuplicateObject Class Reference	137
10.61.1 Detailed Description	137
10.62rpki.exceptions.EmptyPEM Class Reference	138
10.62.1 Detailed Description	138
10.63rpki.exceptions.ForbiddenURI Class Reference	138
10.63.1 Detailed Description	138
10.64rpki.exceptions.HTTPRequestFailed Class Reference	138
10.64.1 Detailed Description	138

10.65rpki.exceptions.HTTPSClientAborted Class Reference	139
10.65.1 Detailed Description	139
10.66rpki.exceptions.MissingCMSCRL Class Reference	139
10.66.1 Detailed Description	139
10.67rpki.exceptions.MissingCMSEECert Class Reference	139
10.67.1 Detailed Description	139
10.68rpki.exceptions.MultipleTLSEECert Class Reference	140
10.68.1 Detailed Description	140
10.69rpki.exceptions.MustBePrefix Class Reference	140
10.69.1 Detailed Description	140
10.70rpki.exceptions.NoActiveCA Class Reference	140
10.70.1 Detailed Description	140
10.71rpki.exceptions.NotACertificateChain Class Reference	141
10.71.1 Detailed Description	141
10.72rpki.exceptions.NotFound Class Reference	141
10.72.1 Detailed Description	141
10.73rpki.exceptions.NotImplementedYet Class Reference	141
10.73.1 Detailed Description	141
10.74rpki.exceptions.NotInDatabase Class Reference	142
10.74.1 Detailed Description	142
10.75rpki.exceptions.ReceivedTLSCACert Class Reference	142
10.75.1 Detailed Description	142
10.76rpki.exceptions.RPKI_Exception Class Reference	142
10.76.1 Detailed Description	143
10.77rpki.exceptions.ServerShuttingDown Class Reference	143
10.77.1 Detailed Description	143
10.78rpki.exceptions.SKIMismatch Class Reference	143
10.78.1 Detailed Description	143
10.79rpki.exceptions.SubprocessError Class Reference	144
10.79.1 Detailed Description	144
10.80rpki.exceptions.TLSValidationError Class Reference	144

10.80.1 Detailed Description	144
10.81rpki.exceptions.UnexpectedCMSCerts Class Reference	144
10.81.1 Detailed Description	145
10.82rpki.exceptions.UnexpectedCMSCRLs Class Reference	145
10.82.1 Detailed Description	145
10.83rpki.exceptions.UnparsableCMSDER Class Reference	145
10.83.1 Detailed Description	145
10.84rpki.exceptions.UpstreamError Class Reference	145
10.84.1 Detailed Description	146
10.85rpki.exceptions.WrongEContentType Class Reference	146
10.85.1 Detailed Description	146
10.86rpki.https.http_client Class Reference	146
10.86.1 Detailed Description	147
10.86.2 Member Function Documentation	147
10.86.3 Member Data Documentation	149
10.87rpki.https.http_listener Class Reference	150
10.87.1 Detailed Description	151
10.87.2 Member Function Documentation	151
10.87.3 Member Data Documentation	152
10.88rpki.https.http_message Class Reference	152
10.88.1 Detailed Description	153
10.88.2 Member Function Documentation	153
10.88.3 Member Data Documentation	154
10.89rpki.https.http_queue Class Reference	155
10.89.1 Detailed Description	156
10.89.2 Member Function Documentation	156
10.89.3 Member Data Documentation	157
10.90rpki.https.http_request Class Reference	158
10.90.1 Detailed Description	158
10.90.2 Member Function Documentation	158
10.90.3 Member Data Documentation	159

10.91rpki.https.http_response Class Reference	159
10.91.1 Detailed Description	160
10.91.2 Member Function Documentation	160
10.91.3 Member Data Documentation	160
10.92rpki.https.http_server Class Reference	161
10.92.1 Detailed Description	161
10.92.2 Member Function Documentation	162
10.92.3 Member Data Documentation	163
10.93rpki.https.http_stream Class Reference	164
10.93.1 Detailed Description	165
10.93.2 Member Function Documentation	165
10.93.3 Member Data Documentation	168
10.94rpki.ipaddrs.v4addr Class Reference	170
10.94.1 Detailed Description	170
10.94.2 Member Function Documentation	170
10.94.3 Member Data Documentation	171
10.95rpki.ipaddrs.v6addr Class Reference	171
10.95.1 Detailed Description	172
10.95.2 Member Function Documentation	172
10.95.3 Member Data Documentation	173
10.96rpki.left_right.bsc_elt Class Reference	173
10.96.1 Detailed Description	174
10.96.2 Member Function Documentation	174
10.96.3 Member Data Documentation	175
10.97rpki.left_right.child_elt Class Reference	177
10.97.1 Detailed Description	177
10.97.2 Member Function Documentation	178
10.97.3 Member Data Documentation	179
10.98rpki.left_right.cms_msg Class Reference	181
10.98.1 Detailed Description	181
10.98.2 Member Data Documentation	181

10.99	rpki.left_right.data_elt Class Reference	182
10.99.1	Detailed Description	182
10.99.2	Member Function Documentation	182
10.99.3	Member Data Documentation	184
10.100	rpki.left_right.left_right_namespace Class Reference	185
10.100.1	Detailed Description	185
10.100.2	Member Data Documentation	185
10.101	rpki.left_right.list_resources_elt Class Reference	186
10.101.1	Detailed Description	186
10.101.2	Member Function Documentation	186
10.101.3	Member Data Documentation	187
10.102	rpki.left_right.list_roa_requests_elt Class Reference	188
10.102.1	Detailed Description	188
10.102.2	Member Function Documentation	189
10.102.3	Member Data Documentation	189
10.103	rpki.left_right.msg Class Reference	190
10.103.1	Detailed Description	190
10.103.2	Member Function Documentation	190
10.103.3	Member Data Documentation	190
10.104	rpki.left_right.parent_elt Class Reference	191
10.104.1	Detailed Description	192
10.104.2	Member Function Documentation	192
10.104.3	Member Data Documentation	193
10.105	rpki.left_right.report_error_elt Class Reference	196
10.105.1	Detailed Description	196
10.105.2	Member Function Documentation	196
10.105.3	Member Data Documentation	197
10.106	rpki.left_right.repository_elt Class Reference	197
10.106.1	Detailed Description	198
10.106.2	Member Function Documentation	198
10.106.3	Member Data Documentation	199

10.107	rpkilib.left_right.route_origin_elt Class Reference	201
10.107.1	Detailed Description	202
10.107.2	Member Function Documentation	202
10.107.3	Member Data Documentation	205
10.108	rpkilib.left_right.sax_handler Class Reference	208
10.108.1	Detailed Description	208
10.108.2	Member Data Documentation	208
10.109	rpkilib.left_right.self_elt Class Reference	209
10.109.1	Detailed Description	210
10.109.2	Member Function Documentation	210
10.109.3	Member Data Documentation	213
10.110	rpkilib.log.logger Class Reference	215
10.110.1	Detailed Description	216
10.110.2	Member Function Documentation	216
10.110.3	Member Data Documentation	216
10.111	rpkilib.manifest.FileAndHash Class Reference	216
10.111.1	Detailed Description	217
10.111.2	Member Function Documentation	217
10.111.3	Member Data Documentation	217
10.112	rpkilib.manifest.FilesAndHashes Class Reference	217
10.112.1	Detailed Description	218
10.112.2	Member Function Documentation	218
10.113	rpkilib.manifest.Manifest Class Reference	218
10.113.1	Detailed Description	218
10.113.2	Member Function Documentation	219
10.113.3	Member Data Documentation	219
10.114	rpkilib.publication.certificate_elt Class Reference	220
10.114.1	Detailed Description	220
10.114.2	Member Data Documentation	220
10.115	rpkilib.publication.client_elt Class Reference	221
10.115.1	Detailed Description	221

10.115.2	Member Function Documentation	221
10.115.3	Member Data Documentation	223
10.116	pkcpublication.cms_msg Class Reference	224
10.116.1	Detailed Description	224
10.116.2	Member Data Documentation	225
10.117	pkcpublication.config_elt Class Reference	225
10.117.1	Detailed Description	226
10.117.2	Member Function Documentation	226
10.117.3	Member Data Documentation	227
10.118	pkcpublication.control_elt Class Reference	228
10.118.1	Detailed Description	228
10.118.2	Member Function Documentation	229
10.119	pkcpublication.crl_elt Class Reference	229
10.119.1	Detailed Description	229
10.119.2	Member Data Documentation	229
10.120	pkcpublication.manifest_elt Class Reference	230
10.120.1	Detailed Description	230
10.120.2	Member Data Documentation	230
10.121	pkcpublication.msg Class Reference	231
10.121.1	Detailed Description	231
10.121.2	Member Function Documentation	231
10.121.3	Member Data Documentation	231
10.122	pkcpublication.publication_namespace Class Reference	232
10.122.1	Detailed Description	232
10.122.2	Member Data Documentation	232
10.123	pkcpublication.publication_object_elt Class Reference	233
10.123.1	Detailed Description	233
10.123.2	Member Function Documentation	234
10.123.3	Member Data Documentation	235
10.124	pkcpublication.report_error_elt Class Reference	235
10.124.1	Detailed Description	236

10.124.2	Member Function Documentation	236
10.124.3	Member Data Documentation	236
10.125	rpki.publication.roa_elt Class Reference	237
10.125.1	Detailed Description	237
10.125.2	Member Data Documentation	237
10.126	rpki.publication.sax_handler Class Reference	238
10.126.1	Detailed Description	238
10.126.2	Member Data Documentation	238
10.127	rpki.resource_set.resource_bag Class Reference	239
10.127.1	Detailed Description	239
10.127.2	Member Function Documentation	240
10.127.3	Member Data Documentation	241
10.128	rpki.resource_set.resource_range Class Reference	242
10.128.1	Detailed Description	243
10.128.2	Member Function Documentation	243
10.128.3	Member Data Documentation	243
10.129	rpki.resource_set.resource_range_as Class Reference	244
10.129.1	Detailed Description	244
10.129.2	Member Function Documentation	244
10.129.3	Member Data Documentation	245
10.130	rpki.resource_set.resource_range_ip Class Reference	245
10.130.1	Detailed Description	246
10.130.2	Member Function Documentation	246
10.131	rpki.resource_set.resource_range_ipv4 Class Reference	247
10.131.1	Detailed Description	247
10.131.2	Member Data Documentation	247
10.132	rpki.resource_set.resource_range_ipv6 Class Reference	248
10.132.1	Detailed Description	248
10.132.2	Member Data Documentation	248
10.133	rpki.resource_set.resource_set Class Reference	248
10.133.1	Detailed Description	249

10.133.2	Member Function Documentation	249
10.133.3	Member Data Documentation	252
10.134	pk resource_set.resource_set_as Class Reference	252
10.134.1	Detailed Description	252
10.134.2	Member Function Documentation	253
10.134.3	Member Data Documentation	253
10.135	pk resource_set.resource_set_ip Class Reference	254
10.135.1	Detailed Description	254
10.135.2	Member Function Documentation	254
10.135.3	Member Data Documentation	255
10.136	pk resource_set.resource_set_ipv4 Class Reference	255
10.136.1	Detailed Description	256
10.136.2	Member Data Documentation	256
10.137	pk resource_set.resource_set_ipv6 Class Reference	256
10.137.1	Detailed Description	257
10.137.2	Member Data Documentation	257
10.138	pk resource_set.roa_prefix Class Reference	257
10.138.1	Detailed Description	258
10.138.2	Member Function Documentation	258
10.138.3	Member Data Documentation	260
10.139	pk resource_set.roa_prefix_ipv4 Class Reference	260
10.139.1	Detailed Description	260
10.139.2	Member Data Documentation	261
10.140	pk resource_set.roa_prefix_ipv6 Class Reference	261
10.140.1	Detailed Description	261
10.140.2	Member Data Documentation	261
10.141	pk resource_set.roa_prefix_set Class Reference	262
10.141.1	Detailed Description	262
10.141.2	Member Function Documentation	262
10.142	pk resource_set.roa_prefix_set_ipv4 Class Reference	264
10.142.1	Detailed Description	264

10.142.	Member Data Documentation	264
10.143.	rpki.resource_set.roa_prefix_set_ipv6 Class Reference	265
10.143.	Detailed Description	265
10.143.	Member Data Documentation	265
10.144.	rpki.roa.ROAIPAddress Class Reference	266
10.144.	Detailed Description	266
10.144.	Member Function Documentation	266
10.144.	Member Data Documentation	266
10.145.	rpki.roa.ROAIPAddresses Class Reference	267
10.145.	Detailed Description	267
10.145.	Member Function Documentation	267
10.146.	rpki.roa.ROAIPAddressFamilies Class Reference	267
10.146.	Detailed Description	267
10.146.	Member Function Documentation	268
10.147.	rpki.roa.ROAIPAddressFamily Class Reference	268
10.147.	Detailed Description	268
10.147.	Member Function Documentation	268
10.147.	Member Data Documentation	269
10.148.	rpki.roa.RouteOriginAttestation Class Reference	269
10.148.	Detailed Description	269
10.148.	Member Function Documentation	269
10.148.	Member Data Documentation	270
10.149.	rpki.rpki_engine.ca_detail_obj Class Reference	270
10.149.	Detailed Description	271
10.149.	Member Function Documentation	272
10.149.	Member Data Documentation	276
10.150.	rpki.rpki_engine.ca_obj Class Reference	278
10.150.	Detailed Description	279
10.150.	Member Function Documentation	279
10.150.	Member Data Documentation	282
10.151.	rpki.rpki_engine.child_cert_obj Class Reference	283

10.151.	Detailed Description	284
10.151.	Member Function Documentation	284
10.151.	Member Data Documentation	286
10.152.	rpki.rpki_engine.revoked_cert_obj Class Reference	287
10.152.	Detailed Description	288
10.152.	Member Function Documentation	288
10.152.	Member Data Documentation	288
10.153.	rpki.rpki_engine.rpkid_context Class Reference	290
10.153.	Detailed Description	290
10.153.	Member Function Documentation	291
10.153.	Member Data Documentation	292
10.154.	rpki.sql.session Class Reference	294
10.154.	Detailed Description	295
10.154.	Member Function Documentation	295
10.154.	Member Data Documentation	297
10.155.	rpki.sql.sql_persistent Class Reference	298
10.155.	Detailed Description	299
10.155.	Member Function Documentation	299
10.155.	Member Data Documentation	303
10.156.	rpki.sql.template Class Reference	304
10.156.	Detailed Description	304
10.156.	Member Function Documentation	305
10.156.	Member Data Documentation	305
10.157.	rpki.sundial.datetime Class Reference	306
10.157.	Detailed Description	307
10.157.	Member Function Documentation	307
10.157.	Member Data Documentation	310
10.158.	rpki.sundial.timedelta Class Reference	310
10.158.	Detailed Description	311
10.158.	Member Function Documentation	311
10.158.	Member Data Documentation	312

10.159	rpkimanager.up_down.base_elt Class Reference	312
10.159.1	Detailed Description	313
10.159.2	Member Function Documentation	313
10.160	rpkimanager.up_down.certificate_elt Class Reference	315
10.160.1	Detailed Description	315
10.160.2	Member Function Documentation	315
10.160.3	Member Data Documentation	316
10.161	rpkimanager.up_down.class_elt Class Reference	317
10.161.1	Detailed Description	317
10.161.2	Member Function Documentation	318
10.161.3	Member Data Documentation	319
10.162	rpkimanager.up_down.class_response_syntax Class Reference	320
10.162.1	Detailed Description	320
10.162.2	Member Function Documentation	321
10.162.3	Member Data Documentation	321
10.163	rpkimanager.up_down.cms_msg Class Reference	321
10.163.1	Detailed Description	322
10.163.2	Member Data Documentation	322
10.164	rpkimanager.up_down.error_response_pdu Class Reference	322
10.164.1	Detailed Description	323
10.164.2	Member Function Documentation	323
10.164.3	Member Data Documentation	324
10.165	rpkimanager.up_down.issue_pdu Class Reference	325
10.165.1	Detailed Description	326
10.165.2	Member Function Documentation	326
10.165.3	Member Data Documentation	327
10.166	rpkimanager.up_down.issue_response_pdu Class Reference	328
10.166.1	Detailed Description	328
10.166.2	Member Function Documentation	328
10.167	rpkimanager.up_down.list_pdu Class Reference	328
10.167.1	Detailed Description	329

10.167.2Member Function Documentation	329
10.168Rpki.up_down.list_response_pdu Class Reference	330
10.168.1Detailed Description	330
10.168.2Member Function Documentation	331
10.168.3Member Data Documentation	332
10.169Rpki.up_down.message_pdu Class Reference	330
10.169.1Detailed Description	331
10.169.2Member Function Documentation	331
10.169.3Member Data Documentation	332
10.170Rpki.up_down.multi_uri Class Reference	333
10.170.1Detailed Description	334
10.170.2Member Function Documentation	334
10.171Rpki.up_down.revoke_pdu Class Reference	335
10.171.1Detailed Description	335
10.171.2Member Function Documentation	335
10.171.3Member Data Documentation	336
10.172Rpki.up_down.revoke_response_pdu Class Reference	336
10.172.1Detailed Description	336
10.173Rpki.up_down.revoke_syntax Class Reference	337
10.173.1Detailed Description	337
10.173.2Member Function Documentation	337
10.173.3Member Data Documentation	338
10.174Rpki.up_down.sax_handler Class Reference	338
10.174.1Detailed Description	338
10.174.2Member Data Documentation	338
10.175Rpki.x509.CMS_object Class Reference	339
10.175.1Detailed Description	340
10.175.2Member Function Documentation	340
10.175.3Member Data Documentation	342
10.176Rpki.x509.CRL Class Reference	344
10.176.1Detailed Description	345
10.176.2Member Function Documentation	345
10.176.3Member Data Documentation	347

10.177	pkix509.DER_CMS_object Class Reference	348
10.177.1	Detailed Description	348
10.177.2	Member Function Documentation	348
10.177.3	Member Data Documentation	349
10.178	pkix509.DER_object Class Reference	349
10.178.1	Detailed Description	350
10.178.2	Member Function Documentation	350
10.178.3	Member Data Documentation	355
10.179	pkix509.PEM_converter Class Reference	356
10.179.1	Detailed Description	356
10.179.2	Member Function Documentation	356
10.179.3	Member Data Documentation	357
10.180	pkix509.PKCS10 Class Reference	358
10.180.1	Detailed Description	358
10.180.2	Member Function Documentation	358
10.180.3	Member Data Documentation	360
10.181	pkix509.ROA Class Reference	361
10.181.1	Detailed Description	361
10.181.2	Member Function Documentation	361
10.181.3	Member Data Documentation	361
10.182	pkix509.RSA Class Reference	362
10.182.1	Detailed Description	363
10.182.2	Member Function Documentation	363
10.182.3	Member Data Documentation	364
10.183	pkix509.RSAPublic Class Reference	365
10.183.1	Detailed Description	366
10.183.2	Member Function Documentation	366
10.183.3	Member Data Documentation	367
10.184	pkix509.SignedManifest Class Reference	367
10.184.1	Detailed Description	368
10.184.2	Member Function Documentation	368

10.184.3	Member Data Documentation	369
10.185	pkix509.X509 Class Reference	369
10.185.1	Detailed Description	370
10.185.2	Member Function Documentation	371
10.185.3	Member Data Documentation	373
10.186	pkix509.XML_CMS_object Class Reference	374
10.186.1	Detailed Description	375
10.186.2	Member Function Documentation	375
10.186.3	Member Data Documentation	376
10.187	pkixml_utils.base_elt Class Reference	377
10.187.1	Detailed Description	378
10.187.2	Member Function Documentation	378
10.187.3	Member Data Documentation	380
10.188	pkixml_utils.data_elt Class Reference	381
10.188.1	Detailed Description	381
10.188.2	Member Function Documentation	381
10.189	pkixml_utils.msg Class Reference	385
10.189.1	Detailed Description	385
10.189.2	Member Function Documentation	385
10.189.3	Member Data Documentation	386
10.190	pkixml_utils.sax_handler Class Reference	386
10.190.1	Detailed Description	387
10.190.2	Member Function Documentation	387
10.190.3	Member Data Documentation	389
10.191	Sequence Class Reference	390
10.192	SequenceOf Class Reference	390
10.193	textwrap.TextWrapper Class Reference	390
10.194	xml.sax.handler.ContentHandler Class Reference	390
11	File Documentation	390
11.1	__init__.py File Reference	390

11.2	async.py File Reference	391
11.3	config.py File Reference	391
11.4	cross_certify.py File Reference	391
11.5	exceptions.py File Reference	392
11.6	https.py File Reference	393
11.7	ipaddrs.py File Reference	394
11.8	irbe_cli.py File Reference	394
11.9	irdbd.py File Reference	396
11.10	left_right.py File Reference	396
11.11	log.py File Reference	397
11.12	manifest.py File Reference	398
11.13	oids.py File Reference	398
11.14	pubd.py File Reference	399
11.15	publication.py File Reference	399
11.16	relaxng.py File Reference	400
11.17	resource_set.py File Reference	400
11.18	roa.py File Reference	401
11.19	rootd.py File Reference	402
11.20	rpki_engine.py File Reference	403
11.21	rpkid.py File Reference	403
11.22	sql.py File Reference	404
11.23	sundial.py File Reference	404
11.24	up_down.py File Reference	405
11.25	x509.py File Reference	405
11.26	xml_utils.py File Reference	406

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.

- <http://codespeak.net/lxml/>. `lxml` in turn requires the Gnome LibXML2 C libraries.
 - FreeBSD: `/usr/ports/devel/py-lxml`
 - Fedora: `python-lxml.i386`
- <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`

[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 copy of the stock OpenSSL 0.9.8g release, 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.

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`
- <http://xmlsoft.org/XSLT/>. Some of the test code uses `xlsltproc`, from the Gnome LibXSLT package.
 - FreeBSD: `/usr/ports/textproc/libxslt`
- <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`

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
- <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
- <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.

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 `rpkid`, `pubd`, `rootd`, and `irdbd`, using the left-right control protocol to set up `rpkid`'s internal state, and setting up a cron job to invoke `rpkid`'s cron action at regular intervals. All other operations should occur either as a result of cron events or as a result of incoming left-right and up-down protocol requests.

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

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

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

All of the daemons use syslog. At present they all set `LOG_ERROR`, 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 [rpkiid](#) traces back to this trust anchor.
- `rpkiid-cert`: Name of file containing [rpkiid](#)'s own BPKI EE certificate.
- `rpkiid-key`: Name of file containing RSA key corresponding to [rpkiid-cert](#).
- `irbe-cert`: Name of file containing BPKI certificate used by IRBE when talking to [rpkiid](#).
- `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.
- `bpki-ta`: Name of file containing master BPKI trust anchor for `pubd`. All BPKI validation in `pubd` traces back to this trust anchor.
- `irbe-cert`: Name of file containing BPKI certificate used by IRBE when talking to `pubd`.
- `pubd-cert`: Name of file containing BPKI certificate used by `pubd`.

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

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 [irbdb](#) traces back to this trust anchor.
- `irbdb-cert`: Name of file containing irdbd's own BPKI certificate.
- `irbdb-key`: Name of file containing RSA key corresponding to irbdb-cert.
- `rpki-cert`: Name of file containing certificate used the one and only by [rpkiid](#) instance authorized to contact this [irbdb](#) instance.
- `https-url`: Service URL for [irbdb](#). 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 2452 2009-05-27 02:54:24Z 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= --verbose

left-right protocol:

parent --action= --tag= --self_id= --parent_id= --bsc_id=
 --repository_id= --peer_contact_uri= --sia_base= --sender_name=
 --recipient_name= --bpki_cms_cert= --bpki_cms_glue=
 --bpki_https_cert= --bpki_https_glue= --rekey --reissue --revoke
 repository --action= --tag= --self_id= --repository_id= --bsc_id=
 --peer_contact_uri= --bpki_cms_cert= --bpki_cms_glue=
 --bpki_https_cert= --bpki_https_glue=
 self --action= --tag= --self_id= --crl_interval= --regen_margin=
 --bpki_cert= --bpki_glue= --rekey --reissue --revoke --run_now
 --publish_world_now
 child --action= --tag= --self_id= --child_id= --bsc_id= --bpki_cert=
 --bpki_glue= --reissue
 route_origin --action= --tag= --self_id= --route_origin_id=
 --as_number= --ipv4= --ipv6= --suppress_publication
 bsc --action= --tag= --self_id= --bsc_id= --key_type= --hash_alg=
 --key_length= --signing_cert= --signing_cert_crl=
 --generate_keypair

publication protocol:

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

Global options (`-config`, `-help`, `-pem_out`) come first, then zero or more commands (`parent`, `repository`, `self`, `child`, `route_origin`, `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.

`-*_id` options refer to the primary keys of previously created objects.

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 rpki'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 irdbd'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`.
- `rpkid-cert`: Name of file containing `rpkid`'s BPKI certificate.
- `https-url`: Service URL for `rpkid`. Must be a `https://` URL.

4.9 testbed.py:

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

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

All of the options in the first (optional) configuration file are just overrides for wired-in default values. In most cases the defaults will suffice, and the set of options is still

in flux, so only a few of the options are described here. The default name for this configuration file is `testbed.conf`, run `testbed` with `"-c filename"` to change it.

`testbed.conf` options:

- `testbed_dir`: Working directory into which `testbed` should write the (many) files it generates. Default is `"testbed.dir"`.
- `irdb_db_pass`: MySQL password for the `"irdb"` user. Default is `"fnord"`. You may want to override this.
- `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_cVPXX0"
```

`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_id" value, one must create a <self/> object before one can usefully configure any other left-right protocol objects.

Every <self/> object has a self_id attribute, which must be specified for the "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_id`, which must be specified for the "get", "set", and "destroy" actions. Every `<bsc/>` also has a `self_id` 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_id`, which must be specified for the "get", "set", and "destroy" actions. Every `<parent/>` also has a `self_id` attribute which

indicates the `<self/>` object with which this `<parent/>` object is associated, a `bsc_id` attribute indicating the `<bsc/>` object to be used when signing messages sent to this parent, and a `repository_id` 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 `parent_id`, which must be specified for the "get", "set", and "destroy" actions. Every `<child/>` also has a `self_id` 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_id`, which must be specified for the "get", "set", and "destroy" actions. Every `<repository/>` also has a `self_id` 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_https_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

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:

- `as_number` (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_id"` attribute naming the `<self/>` that is making the request and also a `"child_id"` 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_id`, and `child_id` 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_id" 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_id" attribute, which is used in responses and must be specified in "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.

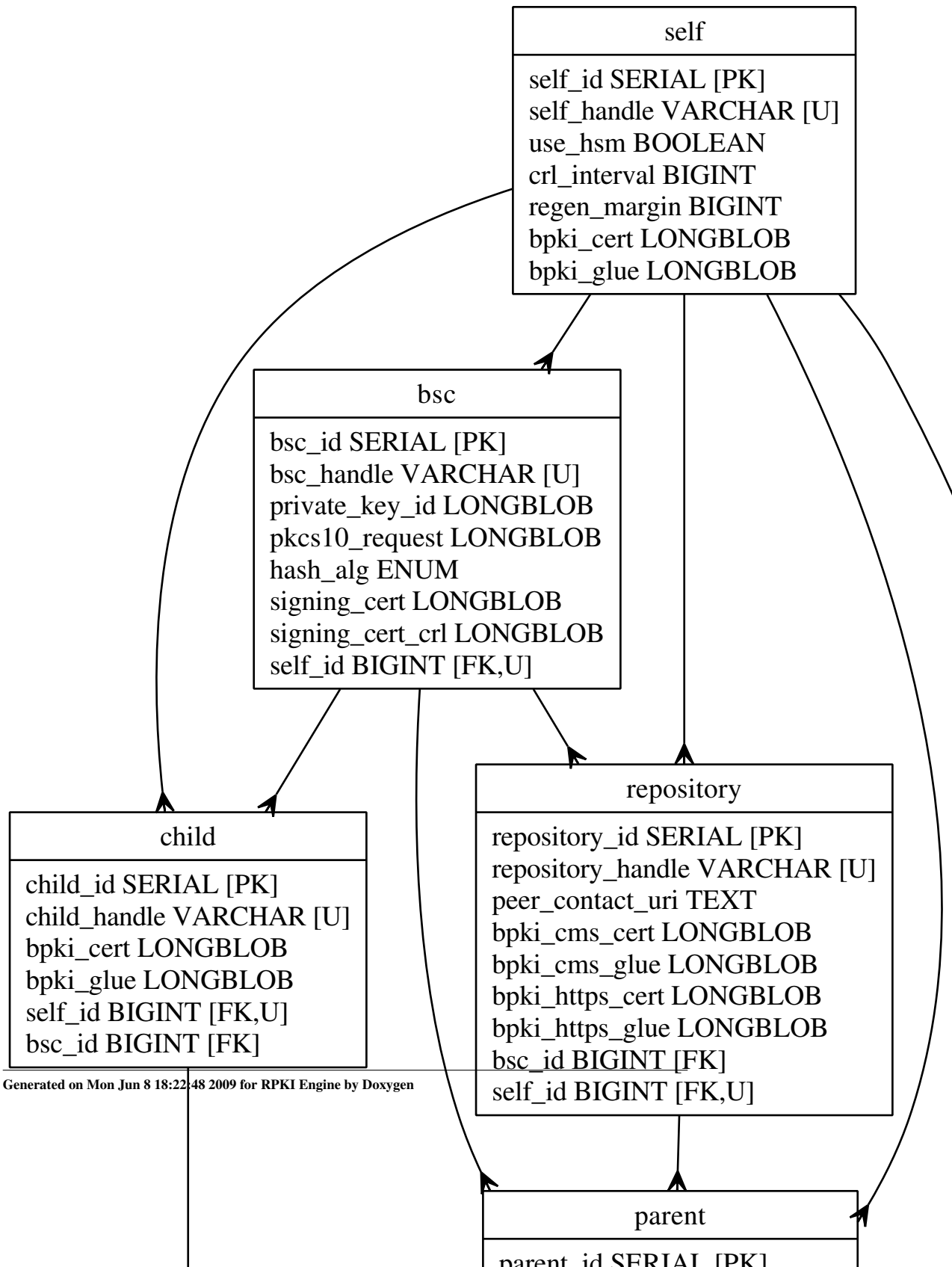
The previous paragraph only covers a "publish" action for a <certificate/> object. For "publish" actions on other objects, the publication server would need to trace permission back to the certificate issued by the parent; for "withdraw" actions, the publication server would have to perform the same 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 rpkiid SQL schema



```
-- $Id: rpkiid.sql 2504 2009-06-08 18:20:54Z 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 route_origin_prefix;
DROP TABLE IF EXISTS route_origin;
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,
    bpki_cms_cert          LONGBLOB,
    bpki_cms_glue          LONGBLOB,
    bpki_https_cert        LONGBLOB,
    bpki_https_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,
    bpki_cms_cert          LONGBLOB,
    bpki_cms_glue          LONGBLOB,
    bpki_https_cert        LONGBLOB,
    bpki_https_glue        LONGBLOB,
    peer_contact_uri       TEXT,
    sia_base               TEXT,
    sender_name            TEXT,
    recipient_name         TEXT,
    self_id                BIGINT UNSIGNED NOT NULL,
    bsc_id                 BIGINT UNSIGNED NOT NULL,
    repository_id          BIGINT UNSIGNED NOT NULL,
    PRIMARY KEY            (parent_id),
    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,
    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,
    bpk_i_cert            LONGBLOB,
    bpk_i_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 route_origin (

```

```

route_origin_id      SERIAL NOT NULL,
route_origin_handle  VARCHAR(255) NOT NULL,
as_number            DECIMAL(24,0),
cert                LONGBLOB,
roa                 LONGBLOB,
self_id             BIGINT UNSIGNED NOT NULL,
ca_detail_id        BIGINT UNSIGNED,
PRIMARY KEY         (route_origin_id),
FOREIGN KEY         (self_id) REFERENCES self (self_id),
FOREIGN KEY         (ca_detail_id) REFERENCES ca_detail (ca_detail_id),
UNIQUE              (self_id, route_origin_handle)
) ENGINE=InnoDB;

CREATE TABLE route_origin_prefix (
  address            VARCHAR(40) NOT NULL,
  prefixlen         TINYINT NOT NULL,
  max_prefixlen     TINYINT NOT NULL,
  version           TINYINT NOT NULL,
  route_origin_id   BIGINT UNSIGNED NOT NULL,
  PRIMARY KEY       (route_origin_id, address, prefixlen, max_prefixlen),
  FOREIGN KEY       (route_origin_id) REFERENCES route_origin (route_origin_id)
) ENGINE=InnoDB;

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

```

7.2 pubd SQL Schema

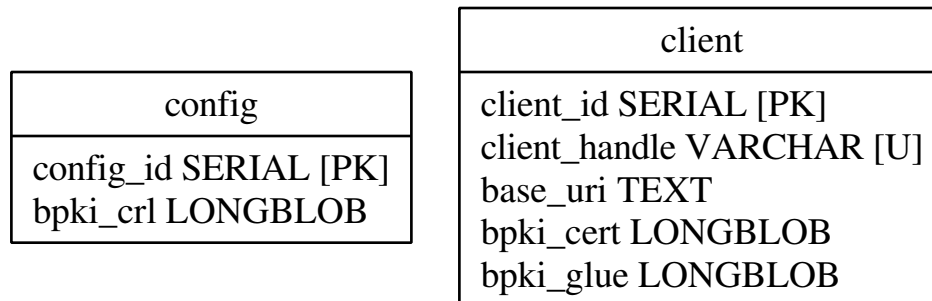


Figure 2: Diagram of pubd.sql

```

-- $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

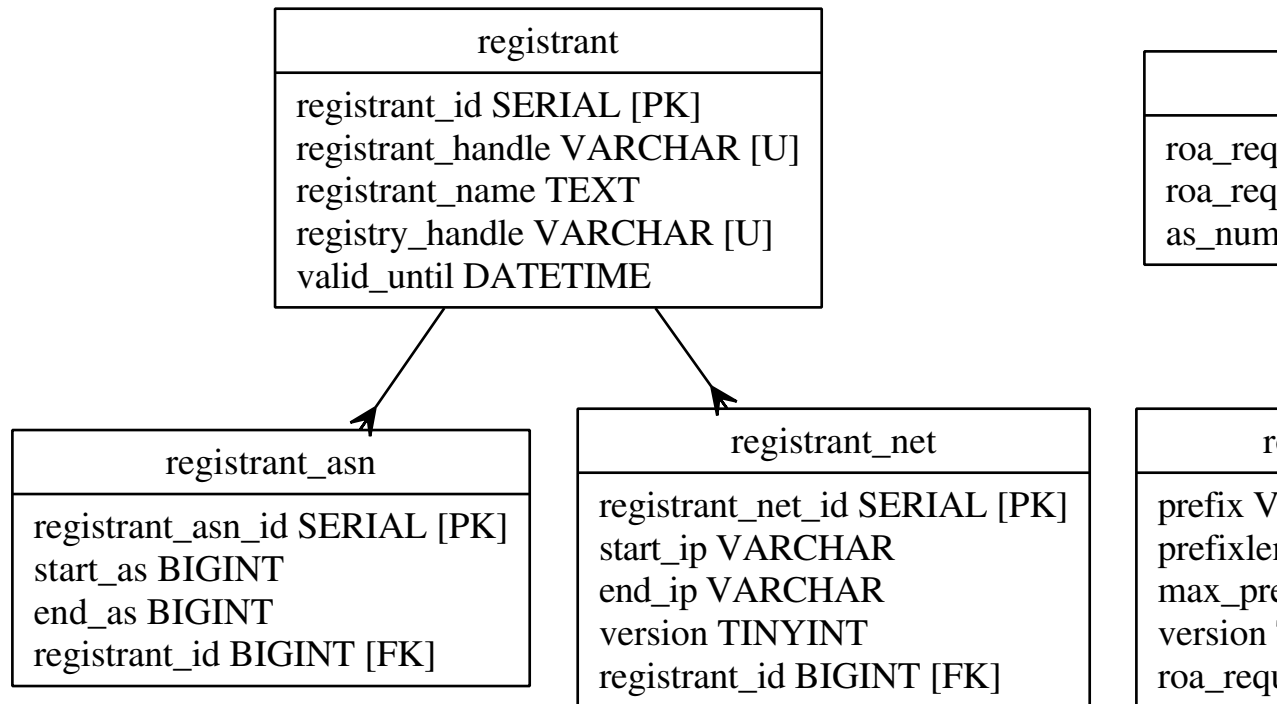


Figure 3: Diagram of irdbd.sql

```

-- $Id: irdbd.sql 2504 2009-06-08 18:20:54Z 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,
    as_number              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".

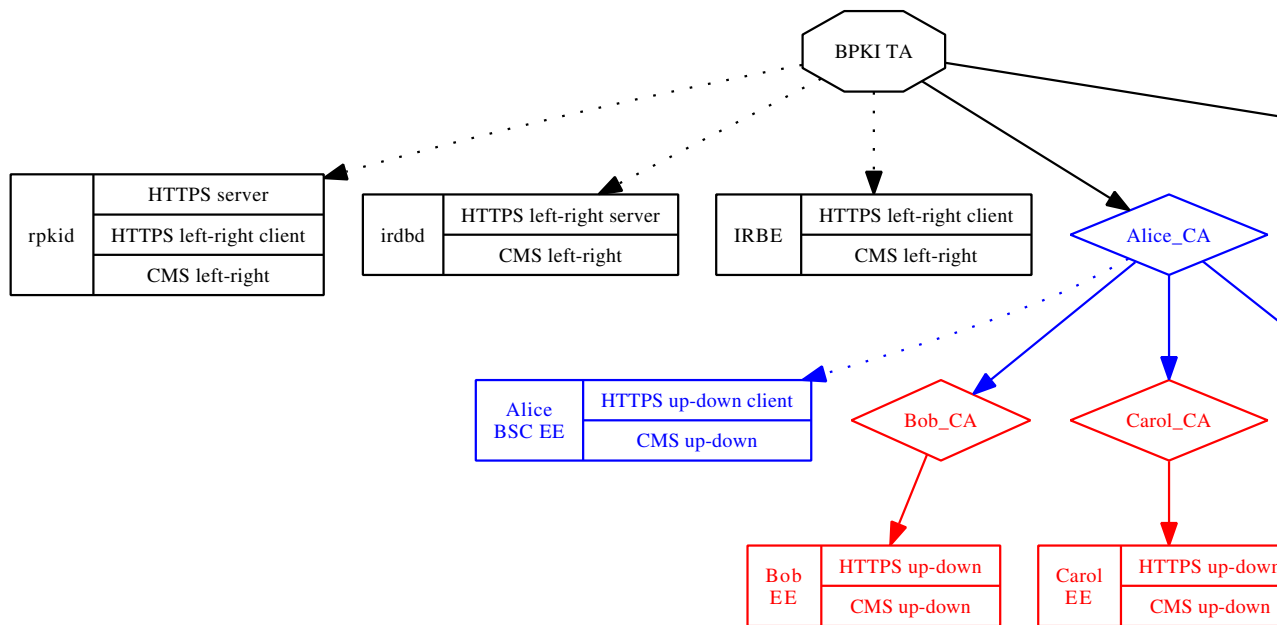
Setup of the BPKI is handled by the back end; for the most part, [rpkid](#) and [pubd](#) just use the result. The one place where the engines are directly involved in creation of new BPKI certificates is in the production of end-entity certificates for use by the engines.

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 **rpkiid** will care about during certificate validation, dotted arrows show the origin of the EE certificates that **rpkiid** uses to sign CMS and TLS messages.

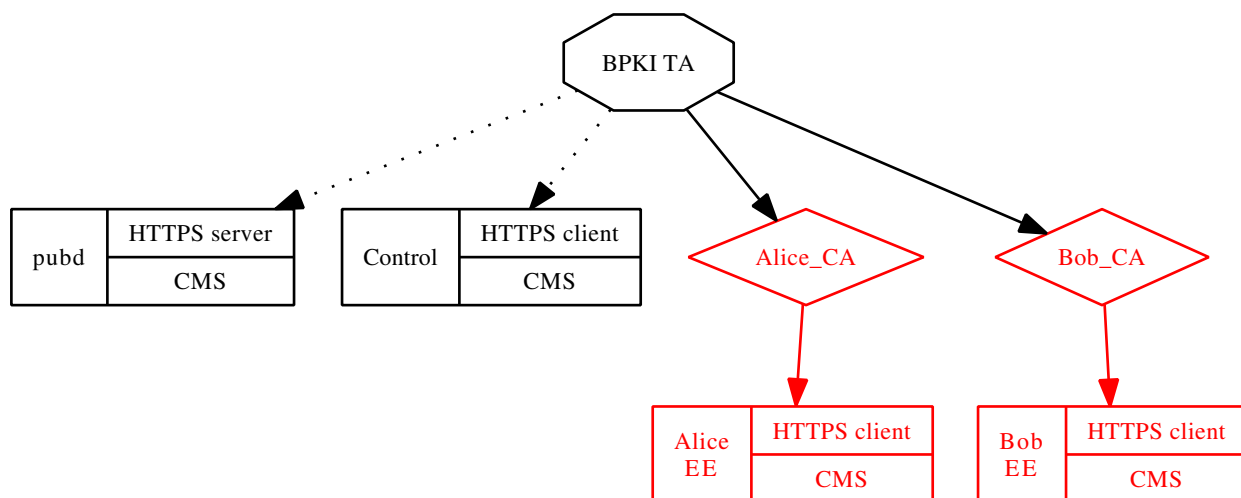
There's one nasty bit where the model had to bend to fit the current state of the underlying protocols: it's not possible to use exactly the same BPKI keys and certificates for HTTPS and CMS. The reason for this is simple: each hosted entity has its own BPKI, as does the hosting entity, but the HTTPS 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 **rpkiid** instance, but is a bit simpler, as **pubd** does not provide hosting in the same sense that **rpkiid** does: **pubd** is a relatively simple server that publishes objects as instructed by its clients.

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



While it is likely that RIRs (at least) will operate both [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 cross_certify

Functions

- def `make_ext`
- def `usage`

Variables

- tuple `cert` = `rpki.x509.X509(POWpkix = x)`
- `child` = None
- `critical` = False,
- tuple `f` = `open(serial_file, "r")`
- `keypair` = None
- tuple `lifetime` = `rpki.sundial.timedelta(days = 30)`
- `notAfter` = `now+lifetime`
- tuple `now` = `rpki.sundial.now()`
- `output` = None
- `parent` = None
- tuple `serial` = `f.read()`
- `serial_file` = None
- tuple `value` = `child.get_SKI()`
- tuple `x` = `POW.pkix.Certificate()`

9.1.1 Detailed Description

Cross-certification tool to issue a new certificate based on an old one that was issued by somebody else. The point of the exercise is to end up with a valid certificate in our own BPKI which has the same subject name and subject public key as the one we're replacing.

```
Usage: 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 (default: stdout) ]
                        [ { -l | --lifetime } timedelta (default: 30 days) ]
```

```
$Id: cross_certify.py 2433 2009-05-16 20:44:12Z 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 cross_certify.make_ext (name, critical, value)`

Definition at line 107 of file cross_certify.py.

9.1.2.2 `def cross_certify.usage (errmsg = None)`

Definition at line 51 of file cross_certify.py.

9.1.3 Variable Documentation

9.1.3.1 `tuple cross_certify.cert = rpki.x509.X509(POWpkix = x)`

Definition at line 132 of file cross_certify.py.

9.1.3.2 `tuple cross_certify::child = None`

Definition at line 59 of file cross_certify.py.

9.1.3.3 cross_certify.critical = False,

Definition at line 122 of file cross_certify.py.

9.1.3.4 tuple cross_certify::f = open(serial_file, "r")

Definition at line 100 of file cross_certify.py.

9.1.3.5 tuple cross_certify::keypair = None

Definition at line 61 of file cross_certify.py.

9.1.3.6 tuple cross_certify::lifetime = rpki.sundial.timedelta(days = 30)

Definition at line 63 of file cross_certify.py.

9.1.3.7 cross_certify.notAfter = now+lifetime

Definition at line 97 of file cross_certify.py.

9.1.3.8 tuple cross_certify.now = rpki.sundial.now()

Definition at line 96 of file cross_certify.py.

9.1.3.9 cross_certify.output = None

Definition at line 64 of file cross_certify.py.

9.1.3.10 tuple cross_certify::parent = None

Definition at line 60 of file cross_certify.py.

9.1.3.11 int cross_certify::serial = f.read()

Definition at line 101 of file cross_certify.py.

9.1.3.12 cross_certify.serial_file = None

Definition at line 62 of file cross_certify.py.

9.1.3.13 tuple cross_certify::value = child.get_SKI()

Definition at line 123 of file cross_certify.py.

9.1.3.14 tuple cross_certify.x = POW.pkix.Certificate()

Definition at line 111 of file cross_certify.py.

9.2 Package irbe_cli**Classes**

- class [bsc_elt](#)
- class [certificate_elt](#)
- class [child_elt](#)
- class [client_elt](#)
- class [cmd_elt_mixin](#)
- class [cmd_msg_mixin](#)
- class [config_elt](#)
- class [crl_elt](#)
- class [left_right_cms_msg](#)
- class [left_right_msg](#)

- class `left_right_sax_handler`
- class `manifest_elt`
- class `parent_elt`
- class `publication_cms_msg`
- class `publication_msg`
- class `publication_sax_handler`
- class `repository_elt`
- class `roa_elt`
- class `route_origin_elt`
- class `self_elt`
- class `UsageWrapper`

Functions

- def `call_daemon`
- def `usage`

Variables

- list `argv` = `sys.argv[1:]`
- tuple `cfg` = `rpki.config.parser(cfg_file, "irbe_cli")`
- string `cfg_file` = `"irbe.conf"`
- tuple `client_cert` = `rpki.x509.X509(Auto_file = cfg.get("rpkid-irbe-cert"))`
- tuple `client_key` = `rpki.x509.RSA(Auto_file = cfg.get("rpkid-irbe-key"))`
- `cms_class` = `left_right_cms_msg`,
- `pem_out` = `None`
- `q_msg` = `q_msg_left_right`
- tuple `q_msg_left_right` = `left_right_msg()`
- tuple `q_msg_publication` = `publication_msg()`
- list `q_pdu` = `left_right_msg.pdus[argv[0]]`
- tuple `server_ta`
- list `top_opts` = `["config=", "help", "pem_out=", "verbose"]`
- tuple `url` = `cfg.get("rpkid-url")`
- tuple `usage_fill` = `UsageWrapper(subsequent_indent = " " * 4)`
- `verbose` = `False`

9.2.1 Detailed Description

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

```
$Id: irbe_cli.py 2452 2009-05-27 02:54:24Z 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 irbe_cli.call_daemon (cms_class, client_key, client_cert, server_ta, url, q_msg)`

Definition at line 249 of file irbe_cli.py.

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

Definition at line 232 of file irbe_cli.py.

9.2.3 Variable Documentation

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

Definition at line 275 of file irbe_cli.py.

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

Definition at line 297 of file irbe_cli.py.

9.2.3.3 irbe_cli.cfg_file = "irbe.conf"

Definition at line 280 of file irbe_cli.py.

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

Definition at line 321 of file irbe_cli.py.

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

Definition at line 320 of file irbe_cli.py.

9.2.3.6 irbe_cli.cms_class = left_right cms_msg,

Definition at line 319 of file irbe_cli.py.

9.2.3.7 irbe_cli.pem_out = None

Definition at line 38 of file irbe_cli.py.

9.2.3.8 irbe_cli.q_msg = q_msg_left_right

Definition at line 308 of file irbe_cli.py.

9.2.3.9 tuple irbe_cli.q_msg_left_right = left_right_msg()

Definition at line 299 of file irbe_cli.py.

9.2.3.10 tuple irbe_cli.q_msg_publication = publication_msg()

Definition at line 302 of file irbe_cli.py.

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

Definition at line 307 of file irbe_cli.py.

9.2.3.12 tuple irbe_cli::server_ta**Initial value:**

```
(rpki.x509.X509(Auto_file = cfg.get("rpkid-bpki-ta")),  
rpki.x509.X509(Auto_file = cfg.get("rpkid-cert")))
```

Definition at line 322 of file irbe_cli.py.

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

Definition at line 230 of file irbe_cli.py.

9.2.3.14 tuple irbe_cli::url = cfg.get("rpkid-url")

Definition at line 324 of file irbe_cli.py.

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

Definition at line 49 of file irbe_cli.py.

9.2.3.16 irbe_cli.verbose = False

Definition at line 281 of file irbe_cli.py.

9.3 Package irdbd**Functions**

- 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](#)
- 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"))

9.3.1 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 2502 2009-06-08 03:56:26Z 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 irdbd.handler (query, path, cb)`

Definition at line 43 of file irdbd.py.

9.3.3 Variable Documentation

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

Definition at line 145 of file irdbd.py.

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

Definition at line 132 of file irdbd.py.

9.3.3.3 irdbd.cfg_file = "irdbd.conf"

Definition at line 120 of file irdbd.py.

9.3.3.4 tuple irdbd.client_ta = (bpki_ta, rpkiid_cert)

Definition at line 161 of file irdbd.py.

9.3.3.5 tuple irdbd.cur = db.cursor()

Definition at line 142 of file irdbd.py.

9.3.3.6 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 138 of file irdbd.py.

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

Definition at line 164 of file irdbd.py.

9.3.3.8 string irdbd.host = "localhost"

Definition at line 162 of file irdbd.py.

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

Definition at line 147 of file irdbd.py.

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

Definition at line 148 of file irdbd.py.

9.3.3.11 `int irdbd.port = 443`

Definition at line 163 of file irdbd.py.

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

Definition at line 146 of file irdbd.py.

9.3.3.13 `irdbd.server_cert = irdbd_cert,`

Definition at line 160 of file irdbd.py.

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

Definition at line 134 of file irdbd.py.

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

Definition at line 150 of file irdbd.py.

9.4 Package pubd

Classes

- class `pubd_context`

Functions

- def `main`

Variables

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

9.4.1 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 2493 2009-06-04 18:30:40Z 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 pubd.main ()`

Definition at line 170 of file pubd.py.

9.4.3 Variable Documentation

9.4.3.1 `pubd.cfg_file = "pubd.conf"`

Definition at line 155 of file pubd.py.

9.4.3.2 `pubd.profile = False`

Definition at line 156 of file pubd.py.

9.5 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 [get_subject_cert](#)
- def [get_subject_pkcs10](#)

- def `issue_subject_cert_maybe`
- 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")`
- tuple `rpki_root_cert` = `rpki.x509.X509`(Auto_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", "Subroot.cer")`
- tuple `rpki_subject_lifetime` = `rpki.sundial.timedelta.parse`(`cfg.get("rpki-subject-lifetime", "30d")`)
- tuple `rpki_subject_pkcs10` = `cfg.get("rpki-subject-pkcs10", "Subroot.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`,

9.5.1 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 2481 2009-06-01 05:07:46Z 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.

9.5.2 Function Documentation

9.5.2.1 `def rootd.compose_response (r_msg)`

Definition at line 147 of file `rootd.py`.

9.5.2.2 `def rootd.del_subject_cert ()`

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

9.5.2.3 def rootd.get_subject_cert ()

Definition at line 46 of file rootd.py.

9.5.2.4 def rootd.get_subject_pkcs10 ()

Definition at line 67 of file rootd.py.

9.5.2.5 def rootd.issue_subject_cert_maybe ()

Definition at line 82 of file rootd.py.

9.5.2.6 def rootd.set_subject_cert (cert)

Definition at line 55 of file rootd.py.

9.5.2.7 def rootd.set_subject_pkcs10 (pkcs10)

Definition at line 76 of file rootd.py.

9.5.2.8 def rootd.up_down_handler (query, path, cb)

Definition at line 202 of file rootd.py.

9.5.3 Variable Documentation**9.5.3.1 tuple rootd.bpki_ta = rpki.x509.X509(Auto_file = cfg.get("bpki-ta"))**

Definition at line 248 of file rootd.py.

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

Definition at line 246 of file rootd.py.

9.5.3.3 rootd.cfg_file = "rootd.conf"

Definition at line 234 of file rootd.py.

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

Definition at line 252 of file rootd.py.

9.5.3.5 tuple rootd.client_ta = (bpki_ta, child_bpki_cert)

Definition at line 276 of file rootd.py.

9.5.3.6 rootd.handlers = up_down_handler)

Definition at line 279 of file rootd.py.

9.5.3.7 rootd.host = https_server_host,

Definition at line 277 of file rootd.py.

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

Definition at line 254 of file rootd.py.

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

Definition at line 255 of file rootd.py.

9.5.3.10 `rootd.port = https_server_port,`

Definition at line 278 of file rootd.py.

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

Definition at line 250 of file rootd.py.

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

Definition at line 251 of file rootd.py.

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

Definition at line 249 of file rootd.py.

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

Definition at line 260 of file rootd.py.

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

Definition at line 257 of file rootd.py.

9.5.3.16 `tuple rootd.rpki_root_cert = rpki.x509.X509(Auto_file =
cfg.get("rpki-root-cert"))`

Definition at line 263 of file rootd.py.

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

Definition at line 264 of file rootd.py.

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

Definition at line 267 of file rootd.py.

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

Definition at line 259 of file rootd.py.

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

Definition at line 262 of file rootd.py.

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

Definition at line 266 of file rootd.py.

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

Definition at line 268 of file rootd.py.

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

Definition at line 271 of file rootd.py.

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

Definition at line 269 of file rootd.py.

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

Definition at line 272 of file rootd.py.

```
9.5.3.26 rootd.server_cert = rootd_bpki_cert,
```

Definition at line 275 of file rootd.py.

9.6 Package rpki

Packages

- package [async](#)
- package [config](#)
- package [exceptions](#)
- package [https](#)
- package [ipaddr](#)
- 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](#)

9.7 Package rpki.async

Classes

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

Functions

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

Variables

- [ExitNow](#) = `asyncore.ExitNow`

9.7.1 Detailed Description

Utilities for event-driven programming.

```
$Id: async.py 2481 2009-06-01 05:07:46Z 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.

9.7.2 Function Documentation

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

Signal handler for `event_loop()`.

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

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

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

Definition at line 219 of file `async.py`.

9.7.2.3 `def rpki.async.exit_event_loop ()`

Force exit from `event_loop()`.

Definition at line 236 of file `async.py`.

9.7.3 Variable Documentation

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

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

9.8 Package rpki.config

Classes

- class [parser](#)

9.8.1 Detailed Description

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

```
$Id: config.py 2452 2009-05-27 02:54:24Z 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.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 [ChildNotFound](#)
- class [ClassNameMismatch](#)
- class [ClassNameUnknown](#)
- class [ClientNotFound](#)
- class [CMSCRLNotSet](#)
- class [CMSVerificationFailed](#)
- class [DBConsistencyError](#)
- class [DERObjectConversionError](#)
- class [DuplicateObject](#)
- class [EmptyPEM](#)
- class [ForbiddenURI](#)
- class [HTTPRequestFailed](#)
- class [HTTPSCientAborted](#)
- class [MissingCMSCRL](#)
- class [MissingCMSEECert](#)
- class [MultipleTLSEECert](#)
- class [MustBePrefix](#)
- class [NoActiveCA](#)
- 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](#)

9.9.1 Detailed Description

Exception definitions for RPKI modules.

\$Id: exceptions.py 2493 2009-06-04 18:30:40Z 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.

9.10 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` = False
- `debug_tls_certs` = False
- tuple `default_http_version` = (1, 0)
- tuple `default_timeout` = `rpki.sundial.timedelta(seconds = 90)`
- string `rpki_content_type` = "application/x-rpki"
- `want_persistent_client` = True
- `want_persistent_server` = True

9.10.1 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 2493 2009-06-04 18:30:40Z 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.

9.10.2 Function Documentation

9.10.2.1 `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 745 of file https.py.

9.10.2.2 **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 687 of file https.py.

9.10.2.3 **def rpki.https.logger (self, msg)**

Definition at line 170 of file https.py.

9.10.2.4 **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 731 of file https.py.

9.10.3 Variable Documentation

9.10.3.1 **dictionary rpki::https.client_queues = {}**

Definition at line 685 of file https.py.

9.10.3.2 **rpki::https.debug = False**

Definition at line 52 of file https.py.

9.10.3.3 rpki::https.debug_tls_certs = False

Definition at line 49 of file https.py.

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

Definition at line 61 of file https.py.

9.10.3.5 tuple rpki::https.default_timeout = rpki.sundial.timedelta(seconds = 90)

Definition at line 59 of file https.py.

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

Definition at line 43 of file https.py.

9.10.3.7 rpki::https.want_persistent_client = True

Definition at line 55 of file https.py.

9.10.3.8 rpki::https.want_persistent_server = True

Definition at line 56 of file https.py.

9.11 Package rpki.ipaddrs**Classes**

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

9.11.1 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.

9.12 Package rpki.left_right

Classes

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

- class [list_resources_elt](#)
- class [list_roa_requests_elt](#)
- class [msg](#)
- class [parent_elt](#)
- class [report_error_elt](#)
- class [repository_elt](#)
- class [route_origin_elt](#)
- class [sax_handler](#)
- class [self_elt](#)

Variables

- [enforce_strict_up_down_xml_sender](#) = False

9.12.1 Detailed Description

RPKI "left-right" protocol.

\$Id: left_right.py 2504 2009-06-08 18:20:54Z 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 Variable Documentation

9.12.2.1 rpki::left_right.enforce_strict_up_down_xml_sender = False

Definition at line 41 of file left_right.py.

9.13 Package rpki.log

Classes

- class `logger`

Functions

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

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)`

9.13.1 Detailed Description

Logging facilities for RPKI libraries.

\$Id: log.py 2452 2009-05-27 02:54:24Z sra \$

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

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

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

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

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

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

9.13.2 Function Documentation

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

Initialize logging system.

Definition at line 50 of file log.py.

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

Enable or disable call tracing.

Definition at line 62 of file log.py.

9.13.2.3 `def rpki.log.trace ()`

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

Definition at line 90 of file log.py.

9.13.3 Variable Documentation

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

Definition at line 88 of file log.py.

9.13.3.2 rpki::log::enable_trace = False

Whether call tracing is enabled.

Definition at line 40 of file log.py.

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

Definition at line 84 of file log.py.

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

Definition at line 87 of file log.py.

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

Definition at line 86 of file log.py.

9.13.3.6 int rpki::log.pid = 0

Definition at line 48 of file log.py.

9.13.3.7 string rpki::log.tag = ""

Definition at line 47 of file log.py.

9.13.3.8 rpki::log::use_syslog = False

Whether to use syslog.

Definition at line 45 of file log.py.

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

Definition at line 85 of file log.py.

9.14 Package rpki.manifest**Classes**

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

9.14.1 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.

9.15 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.

9.15.1 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.

9.15.2 Variable Documentation

9.15.2.1 `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.

9.15.2.2 `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.

9.16 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](#)

Variables

- tuple [obj2elt](#) = dict((e.payload_type, e) for e in ([certificate_elt](#), [crl_elt](#), [manifest_elt](#), [roa_elt](#)))

Map of data types to [publication](#) element wrapper types.

9.16.1 Detailed Description

RPKI "publication" protocol.

\$Id: publication.py 2493 2009-06-04 18:30:40Z 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.

9.16.2 Variable Documentation

9.16.2.1 `rpki::publication::obj2elt = dict((e.payload_type, e) for e in (certificate_elt, crl_elt, manifest_elt, roa_elt))`

Map of data types to [publication](#) element wrapper types.

Definition at line 280 of file `publication.py`.

9.17 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.

9.17.1 Variable Documentation

9.17.1.1 `rpki::relaxng::left_right`

Parsed RelaxNG [left_right](#) schema.

Definition at line 7 of file `relaxng.py`.

9.17.1.2 `rpki::relaxng::publication`

Parsed RelaxNG [publication](#) schema.

Definition at line 1259 of file `relaxng.py`.

9.17.1.3 `rpki::relaxng::up_down`

Parsed RelaxNG [up_down](#) schema.

Definition at line 1005 of file relaxng.py.

9.18 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.

9.18.1 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 2457 2009-05-28 18:21:06Z 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.

9.18.2 Function Documentation

9.18.2.1 `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 499 of file `resource_set.py`.

9.18.2.2 `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 511 of file resource_set.py.

9.18.2.3 `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.

9.18.2.4 `def rpki.resource_set.test1 (t, s1, s2)`

Definition at line 868 of file resource_set.py.

9.18.2.5 `def rpki.resource_set.test2 (t, s1, s2)`

Definition at line 901 of file resource_set.py.

9.18.3 Variable Documentation

9.18.3.1 `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.

9.19 Package rpki.roa

Classes

- class [ROAIPAddress](#)

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

9.19.1 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
```

9.20 Package rpki.rpki_engine

Classes

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

9.20.1 Detailed Description

Global context for rpkid.

\$Id: rpki_engine.py 2502 2009-06-08 03:56:26Z 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.sql

Classes

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

9.21.1 Detailed Description

SQL interface code.

\$Id: sql.py 2502 2009-06-08 03:56:26Z 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 Package rpki.sundial

Classes

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

Functions

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

9.22.1 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.

```
$Id: sundial.py 2452 2009-05-27 02:54:24Z 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 Function Documentation

9.22.2.1 def rpki.sundial.now ()

Get current timestamp.

Definition at line 41 of file sundial.py.

9.22.2.2 def rpki.sundial.test (t)

Definition at line 227 of file sundial.py.

9.23 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/"

9.23.1 Detailed Description

RPKI "up-down" protocol.

\$Id: up_down.py 2499 2009-06-07 01:04:39Z 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 Variable Documentation

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

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

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

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

9.24 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](#)

9.24.1 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 2496 2009-06-05 01:57:44Z 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.

9.24.2 Function Documentation

9.24.2.1 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.

9.24.2.2 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 655 of file x509.py.

9.25 Package rpki.xml_utils

Classes

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

9.25.1 Detailed Description

XML utilities.

\$Id: xml_utils.py 2493 2009-06-04 18:30:40Z 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.

9.26 Package rpkiid

Functions

- def [main](#)

Variables

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

9.26.1 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 2452 2009-05-27 02:54:24Z 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.

9.26.2 Function Documentation

9.26.2.1 `def rpkid.main ()`

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

9.26.3 Variable Documentation

9.26.3.1 `rpkid.cfg_file = "rpkid.conf"`

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

9.26.3.2 `rpkid.profile = None`

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

10 Class Documentation

10.1 `asynchat.async_chat` Class Reference

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

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

- [https.py \(2493\)](#)

10.2 `asyncore.dispatcher` Class Reference

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

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

- [https.py \(2493\)](#)

10.3 `ConfigParser.RawConfigParser` Class Reference

Inherited by [rpki.config.parser](#).

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

- [config.py \(2452\)](#)

10.4 Exception Class Reference

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

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

- [exceptions.py \(2493\)](#)

10.5 `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.

10.5.1 Detailed Description

Definition at line 143 of file `irbe_cli.py`.

10.5.2 Member Function Documentation

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

`--signing_cert option.`

Definition at line 147 of file `irbe_cli.py`.

10.5.2.2 `def irbe_cli.bsc_elt.client_query_signing_cert_crl (self, arg)`

`--signing_cert_crl option.`

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

10.5.2.3 `def irbe_cli.bsc_elt.client_reply_decode (self)`

Reimplemented from `irbe_cli.cmd_elt_mixin`.

Definition at line 155 of file `irbe_cli.py`.

10.5.3 Member Data Documentation

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

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

At the moment the only such is the `bsc.pkcs10_request` sub-element, but writing this generally is no harder than handling that one special case.

Reimplemented from [irbe_cli.cmd_elt_mixin](#).

Definition at line 145 of file `irbe_cli.py`.

10.5.3.2 `irbe_cli.bsc_elt.signing_cert`

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

Definition at line 149 of file `irbe_cli.py`.

10.5.3.3 `irbe_cli.bsc_elt.signing_cert_crl`

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

Definition at line 153 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2452\)](#)

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 206 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2452\)](#)

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 165 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2452\)](#)

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 203 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2452\)](#)

10.9 `irbe_cli.cmd_elt_mixin` Class Reference

Inherits [object](#).

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.manifest_elt](#), [irbe_cli.parent_elt](#), [irbe_cli.repository_elt](#), [irbe_cli.roa_elt](#), [irbe_cli.route_origin_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 [client_reply_decode](#)
- def [client_reply_show](#)
- 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.

10.9.1 Detailed Description

Protocol mix-in for command line client element PDUs.

Definition at line 51 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 75 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 92 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 100 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 108 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 104 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 96 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 112 of file irbe_cli.py.

10.9.2.8 def irbe_cli.cmd_elt_mixin.client_reply_decode (self)

Reimplemented in [irbe_cli.bsc_elt](#).

Definition at line 116 of file irbe_cli.py.

10.9.2.9 def irbe_cli.cmd_elt_mixin.client_reply_show (self)

Definition at line 119 of file irbe_cli.py.

10.9.2.10 def irbe_cli.cmd_elt_mixin.usage (cls)

Generate usage message for this PDU.

Definition at line 64 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 94 of file irbe_cli.py.

10.9.3.2 irbe_cli.cmd_elt_mixin.bpki_cms_cert

Definition at line 102 of file irbe_cli.py.

10.9.3.3 irbe_cli.cmd_elt_mixin.bpki_cms_glue

Definition at line 106 of file irbe_cli.py.

10.9.3.4 irbe_cli.cmd_elt_mixin.bpki_glue

Definition at line 98 of file irbe_cli.py.

10.9.3.5 irbe_cli.cmd_elt_mixin.bpki_https_cert

Definition at line 110 of file irbe_cli.py.

10.9.3.6 irbe_cli.cmd_elt_mixin.bpki_https_glue

Definition at line 114 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.

At the moment the only such is the `bsc.pkcs10_request` sub-element, but writing this generally is no harder than handling that one special case.

Reimplemented in [irbe_cli.bsc_elt](#).

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

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

- [irbe_cli.py \(2452\)](#)

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 125 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 131 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2452\)](#)

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 197 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 199 of file `irbe_cli.py`.

10.11.3 Member Data Documentation

10.11.3.1 `irbe_cli.config_elt.bpki_crl`

Definition at line 201 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2452\)](#)

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 209 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2452\)](#)

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 192 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 193 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2452\)](#)

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 185 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, route_origin_elt))
```

Dispatch table of PDUs for this protocol.

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

Definition at line 186 of file irbe_cli.py.

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

- [irbe_cli.py \(2452\)](#)

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 189 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 190 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2452\)](#)

10.16 `irbe_cli.manifest_elt` Class Reference

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

10.16.1 Detailed Description

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

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

- [irbe_cli.py \(2452\)](#)

10.17 `irbe_cli.parent_elt` Class Reference

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

10.17.1 Detailed Description

Definition at line 162 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2452\)](#)

10.18 `irbe_cli.publication_cms_msg` Class Reference

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

Static Public Attributes

- `saxify` = `publication_sax_handler.saxify`

10.18.1 Detailed Description

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

10.18.2 Member Data Documentation

10.18.2.1 irbe_cli.publication_cms_msg.saxify = publication_sax_handler.saxify [static]

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

Definition at line 226 of file irbe_cli.py.

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

- [irbe_cli.py \(2452\)](#)

10.19 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.

10.19.1 Detailed Description

Definition at line 218 of file irbe_cli.py.

10.19.2 Member Data Documentation

10.19.2.1 tuple irbe_cli.publication_msg.pdus [static]

Initial value:

```
dict((x.element_name, x)
      for x in (config_elt, client_elt, certificate_elt, srl_elt, manifest_elt, roa_elt))
```

Dispatch table of PDUs for this protocol.

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

Definition at line 219 of file irbe_cli.py.

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

- [irbe_cli.py \(2452\)](#)

10.20 `irbe_cli.publication_sax_handler` Class Reference

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

Static Public Attributes

- `pdu = publication_msg`

10.20.1 Detailed Description

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

10.20.2 Member Data Documentation

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

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

Definition at line 223 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2452\)](#)

10.21 `irbe_cli.repository_elt` Class Reference

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

10.21.1 Detailed Description

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

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

- [irbe_cli.py \(2452\)](#)

10.22 `irbe_cli.roa_elt` Class Reference

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

10.22.1 Detailed Description

Definition at line 215 of file irbe_cli.py.

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

- [irbe_cli.py \(2452\)](#)

10.23 irbe_cli.route_origin_elt Class Reference

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

Public Member Functions

- def [client_query_as_number](#)
- def [client_query_ipv4](#)
- def [client_query_ipv6](#)

Public Attributes

- [as_number](#)
- [ipv4](#)
- [ipv6](#)

10.23.1 Detailed Description

Definition at line 171 of file irbe_cli.py.

10.23.2 Member Function Documentation

10.23.2.1 def irbe_cli.route_origin_elt.client_query_as_number (*self*, *arg*)

Handle autonomous sequence numbers.

Definition at line 173 of file irbe_cli.py.

10.23.2.2 `def irbe_cli.route_origin_elt.client_query_ipv4 (self, arg)`

Handle IPv4 addresses.

Definition at line 177 of file `irbe_cli.py`.

10.23.2.3 `def irbe_cli.route_origin_elt.client_query_ipv6 (self, arg)`

Handle IPv6 addresses.

Definition at line 181 of file `irbe_cli.py`.

10.23.3 Member Data Documentation

10.23.3.1 `irbe_cli.route_origin_elt.as_number`

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

Definition at line 175 of file `irbe_cli.py`.

10.23.3.2 `irbe_cli.route_origin_elt.ipv4`

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

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

10.23.3.3 `irbe_cli.route_origin_elt.ipv6`

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

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

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

- [irbe_cli.py \(2452\)](#)

10.24 `irbe_cli.self_elt` Class Reference

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

10.24.1 Detailed Description

Definition at line 140 of file `irbe_cli.py`.

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

- [irbe_cli.py \(2452\)](#)

10.25 `irbe_cli.UsageWrapper` Class Reference

Inherits [textwrap::TextWrapper](#).

Public Member Functions

- `def __call__`

10.25.1 Detailed Description

Call interface around Python `textwrap.TextWrapper` class.

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

10.25.2 Member Function Documentation

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

Format arguments, with `TextWrapper` indentation.

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

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

- [irbe_cli.py \(2452\)](#)

10.26 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 \(2424\)](#)

10.27 object Class Reference

Inherited by [irbe_cli.cmd_elt_mixin](#), [irbe_cli.cmd_msg_mixin](#), [pubd.pubd_context](#), [rpki.async.iterator](#), [rpki.async.timer](#), [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 \(2496\)](#)

10.28 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.

10.28.1 Detailed Description

A container for various pubd parameters.

Definition at line 46 of file pubd.py.

10.28.2 Member Function Documentation

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

Definition at line 51 of file pubd.py.

10.28.2.2 def pubd.pubd_context.build_https_ta_cache (self)

Build dynamic TLS trust anchors.

Definition at line 138 of file pubd.py.

10.28.2.3 def pubd.pubd_context.clear_https_ta_cache (self)

Clear dynamic TLS trust anchors.

Definition at line 130 of file pubd.py.

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

Process one PDU from a client.

Definition at line 98 of file pubd.py.

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

Process one PDU from the IRBE.

Definition at line 78 of file pubd.py.

**10.28.2.6 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.

10.28.3 Member Data Documentation**10.28.3.1 pubd.pubd_context.bpki_ta**

Definition at line 55 of file pubd.py.

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

Definition at line 96 of file pubd.py.

10.28.3.3 pubd.pubd_context.https_server_host

Definition at line 60 of file pubd.py.

10.28.3.4 pubd.pubd_context.https_server_port

Definition at line 61 of file pubd.py.

10.28.3.5 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.

10.28.3.6 pubd.pubd_context.irbe_cert

Definition at line 56 of file pubd.py.

10.28.3.7 pubd.pubd_context.pubd_cert

Definition at line 57 of file pubd.py.

10.28.3.8 pubd.pubd_context.pubd_key

Definition at line 58 of file pubd.py.

10.28.3.9 pubd.pubd_context.publication_base

Definition at line 63 of file pubd.py.

10.28.3.10 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 \(2493\)](#)

10.29 pydatetime.datetime Class Reference

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

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

- [sundial.py \(2452\)](#)

10.30 pydatetime.timedelta Class Reference

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

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

- [sundial.py \(2452\)](#)

10.31 rootd.cms_msg Class Reference

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

Static Public Attributes

- [saxify](#) = sax_handler.saxify

10.31.1 Detailed Description

Definition at line 199 of file rootd.py.

10.31.2 Member Data Documentation

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

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

Definition at line 200 of file rootd.py.

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

- [rootd.py \(2481\)](#)

10.32 rootd.issue_pdu Class Reference

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

Public Member Functions

- def [serve_pdu](#)

10.32.1 Detailed Description

Definition at line 166 of file rootd.py.

10.32.2 Member Function Documentation

10.32.2.1 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 167 of file rootd.py.

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

- [rootd.py](#) (2481)

10.33 rootd.list_pdu Class Reference

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

Public Member Functions

- def [serve_pdu](#)

10.33.1 Detailed Description

Definition at line 160 of file rootd.py.

10.33.2 Member Function Documentation

10.33.2.1 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 161 of file rootd.py.

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

- [rootd.py \(2481\)](#)

10.34 rootd.message_pdu Class Reference

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

Static Public Attributes

- dictionary [name2type](#)
- tuple [type2name](#) = dict((v, k) for k, v in name2type.items())

10.34.1 Detailed Description

Definition at line 185 of file rootd.py.

10.34.2 Member Data Documentation

10.34.2.1 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 186 of file rootd.py.

```
10.34.2.2 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 194 of file rootd.py.

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

- [rootd.py \(2481\)](#)

10.35 rootd.revoke_pdu Class Reference

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

Public Member Functions

- def [serve_pdu](#)

10.35.1 Detailed Description

Definition at line 174 of file rootd.py.

10.35.2 Member Function Documentation

10.35.2.1 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 175 of file rootd.py.

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

- [rootd.py \(2481\)](#)

10.36 rootd.sax_handler Class Reference

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

Static Public Attributes

- [pdu](#) = [message_pdu](#)

10.36.1 Detailed Description

Definition at line 196 of file rootd.py.

10.36.2 Member Data Documentation

10.36.2.1 rootd.sax_handler.pdu = message_pdu [static]

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

Definition at line 197 of file rootd.py.

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

- [rootd.py](#) (2481)

10.37 rpki.async.iterator Class Reference

Inherits [object](#).

Public Member Functions

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

Public Attributes

- [caller_function](#)
- [done_callback](#)
- [item_callback](#)
- [iterator](#)

10.37.1 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`.

10.37.2 Member Function Documentation

10.37.2.1 `def rpki.async.iterator.__call__ (self, args)`

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

10.37.2.2 `def rpki.async.iterator.__init__ (self, iterable, item_callback, done_callback)`

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

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

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

10.37.2.4 `def rpki.async.iterator.ignore (self, ignored)`

Definition at line 74 of file `async.py`.

10.37.3 Member Data Documentation

10.37.3.1 `rpki.async.iterator.caller_function`

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

10.37.3.2 `rpki.async.iterator.done_callback`

Definition at line 47 of file `async.py`.

10.37.3.3 `rpki.async.iterator.item_callback`

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

10.37.3.4 `rpki.async.iterator.iterator`

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

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

- [async.py \(2481\)](#)

10.38 `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).

10.38.1 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 77 of file `async.py`.

10.38.2 Member Function Documentation

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

Definition at line 121 of file `async.py`.

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

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

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

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

10.38.2.4 `def rpki.async.timer.cancel (self)`

Cancel a timer, if it was set.

Definition at line 124 of file `async.py`.

10.38.2.5 `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 206 of file `async.py`.

10.38.2.6 `def rpki.async.timer.errback (self, e)`

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

Definition at line 154 of file `async.py`.

10.38.2.7 `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 137 of file `async.py`.

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

Test whether this timer is currently set.

Definition at line 133 of file async.py.

10.38.2.9 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 166 of file async.py.

10.38.2.10 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 184 of file async.py.

10.38.2.11 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 103 of file async.py.

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

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

Definition at line 161 of file `async.py`.

10.38.2.13 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 144 of file `async.py`.

10.38.3 Member Data Documentation**10.38.3.1 rpki.async.timer.errback**

Definition at line 163 of file `async.py`.

10.38.3.2 rpki.async.timer.handler

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

10.38.3.3 rpki::async.timer::queue = [] [static]

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

Definition at line 95 of file `async.py`.

10.38.3.4 rpki.async.timer.when

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

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

- [async.py \(2481\)](#)

10.39 rpki.config.parser Class Reference

Inherits [ConfigParser::RawConfigParser](#).

Public Member Functions

- def [__init__](#)
- def [get](#)
- def [multiget](#)

Public Attributes

- [default_section](#)

10.39.1 Detailed Description

Definition at line 38 of file `config.py`.

10.39.2 Member Function Documentation

10.39.2.1 def rpki.config.parser.__init__ (*self*, *filename* = None, *section* = None)

Initialize this parser.

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

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

Get an option, perhaps with a default value.

Definition at line 67 of file config.py.

10.39.2.3 `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 49 of file config.py.

10.39.3 Member Data Documentation

10.39.3.1 `rpki.config.parser.default_section`

Definition at line 47 of file config.py.

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

- [config.py \(2452\)](#)

10.40 rpki.exceptions.BadClassNameSyntax Class Reference

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

10.40.1 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 \(2493\)](#)

10.41 `rpki.exceptions.BadClientURL` Class Reference

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

10.41.1 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 \(2493\)](#)

10.42 `rpki.exceptions.BadContactURL` Class Reference

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

10.42.1 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 \(2493\)](#)

10.43 `rpki.exceptions.BadExtension` Class Reference

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

10.43.1 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 \(2493\)](#)

10.44 `rpki.exceptions.BadIRDBReply` Class Reference

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

10.44.1 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 \(2493\)](#)

10.45 `rpki.exceptions.BadIssueResponse` Class Reference

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

10.45.1 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 \(2493\)](#)

10.46 `rpki.exceptions.BadPKCS10` Class Reference

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

10.46.1 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 \(2493\)](#)

10.47 `rpki.exceptions.BadPublicationReply` Class Reference

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

10.47.1 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 \(2493\)](#)

10.48 `rpki.exceptions.BadQuery` Class Reference

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

10.48.1 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 \(2493\)](#)

10.49 `rpki.exceptions.BadSender` Class Reference

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

10.49.1 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 \(2493\)](#)

10.50 `rpki.exceptions.BadStatusCode` Class Reference

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

10.50.1 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 \(2493\)](#)

10.51 `rpki.exceptions.BadURISyntax` Class Reference

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

10.51.1 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 \(2493\)](#)

10.52 `rpki.exceptions.BSCNotFound` Class Reference

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

10.52.1 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 \(2493\)](#)

10.53 `rpki.exceptions.ChildNotFound` Class Reference

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

10.53.1 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 \(2493\)](#)

10.54 `rpki.exceptions.ClassNameMismatch` Class Reference

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

10.54.1 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 \(2493\)](#)

10.55 `rpki.exceptions.ClassNameUnknown` Class Reference

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

10.55.1 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 \(2493\)](#)

10.56 `rpki.exceptions.ClientNotFound` Class Reference

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

10.56.1 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 \(2493\)](#)

10.57 `rpki.exceptions.CMSCRLNotSet` Class Reference

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

10.57.1 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 \(2493\)](#)

10.58 `rpki.exceptions.CMSVerificationFailed` Class Reference

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

10.58.1 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 \(2493\)](#)

10.59 `rpki.exceptions.DBConsistencyError` Class Reference

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

10.59.1 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 \(2493\)](#)

10.60 `rpki.exceptions.DERObjectConversionError` Class Reference

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

10.60.1 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 \(2493\)](#)

10.61 `rpki.exceptions.DuplicateObject` Class Reference

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

10.61.1 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 \(2493\)](#)

10.62 `rpki.exceptions.EmptyPEM` Class Reference

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

10.62.1 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 \(2493\)](#)

10.63 `rpki.exceptions.ForbiddenURI` Class Reference

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

10.63.1 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 \(2493\)](#)

10.64 `rpki.exceptions.HTTPRequestFailed` Class Reference

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

10.64.1 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 \(2493\)](#)

10.65 `rpki.exceptions.HTTPSClientAborted` Class Reference

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

10.65.1 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 \(2493\)](#)

10.66 `rpki.exceptions.MissingCMSCRL` Class Reference

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

10.66.1 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 \(2493\)](#)

10.67 `rpki.exceptions.MissingCMSEECert` Class Reference

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

10.67.1 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 \(2493\)](#)

10.68 `rpki.exceptions.MultipleTLSEECert` Class Reference

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

10.68.1 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 \(2493\)](#)

10.69 `rpki.exceptions.MustBePrefix` Class Reference

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

10.69.1 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 \(2493\)](#)

10.70 `rpki.exceptions.NoActiveCA` Class Reference

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

10.70.1 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 \(2493\)](#)

10.71 `rpki.exceptions.NotACertificateChain` Class Reference

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

10.71.1 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 \(2493\)](#)

10.72 `rpki.exceptions.NotFound` Class Reference

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

10.72.1 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 \(2493\)](#)

10.73 `rpki.exceptions.NotImplementedYet` Class Reference

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

10.73.1 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 \(2493\)](#)

10.74 rpki.exceptions.NotInDatabase Class Reference

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

10.74.1 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 \(2493\)](#)

10.75 rpki.exceptions.ReceivedTLSCACert Class Reference

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

10.75.1 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 \(2493\)](#)

10.76 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.ChildNotFound](#),
[rpki.exceptions.ClassNameMismatch](#), [rpki.exceptions.ClassNameUnknown](#),
[rpki.exceptions.ClientNotFound](#), [rpki.exceptions.CMSURLNotSet](#),
[rpki.exceptions.CMSVerificationFailed](#), [rpki.exceptions.DBConsistencyError](#),
[rpki.exceptions.DERObjectConversionError](#), [rpki.exceptions.DuplicateObject](#),
[rpki.exceptions.EmptyPEM](#), [rpki.exceptions.ForbiddenURI](#),

<code>rpki.exceptions.HTTPRequestFailed,</code>	<code>rpki.exceptions.HTTPSClientAborted,</code>
<code>rpki.exceptions.MissingCMSCRL,</code>	<code>rpki.exceptions.MissingCMSEECert,</code>
<code>rpki.exceptions.MustBePrefix,</code>	<code>rpki.exceptions.NoActiveCA,</code>
<code>rpki.exceptions.NotACertificateChain,</code>	<code>rpki.exceptions.NotFound,</code>
<code>rpki.exceptions.NotImplementedYet,</code>	<code>rpki.exceptions.NotInDatabase,</code>
<code>rpki.exceptions.ServerShuttingDown,</code>	<code>rpki.exceptions.SKIMismatch,</code>
<code>rpki.exceptions.SubprocessError,</code>	<code>rpki.exceptions.TLSValidationError,</code>
<code>rpki.exceptions.UnexpectedCMSCerts,</code>	<code>rpki.exceptions.UnexpectedCMSCRLs,</code>
<code>rpki.exceptions.UnparsableCMSDER,</code>	<code>rpki.exceptions.UpstreamError,</code>
<code>rpki.exceptions.WrongEContentType.</code>	<code>and</code>

10.76.1 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 \(2493\)](#)

10.77 `rpki.exceptions.ServerShuttingDown` Class Reference

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

10.77.1 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 \(2493\)](#)

10.78 `rpki.exceptions.SKIMismatch` Class Reference

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

10.78.1 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 \(2493\)](#)

10.79 `rpki.exceptions.SubprocessError` Class Reference

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

10.79.1 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 \(2493\)](#)

10.80 `rpki.exceptions.TLSValidationError` Class Reference

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

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

10.80.1 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 \(2493\)](#)

10.81 `rpki.exceptions.UnexpectedCMSCerts` Class Reference

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

10.81.1 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 \(2493\)](#)

10.82 `rpki.exceptions.UnexpectedCMSCRLs` Class Reference

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

10.82.1 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 \(2493\)](#)

10.83 `rpki.exceptions.UnparsableCMSDER` Class Reference

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

10.83.1 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 \(2493\)](#)

10.84 `rpki.exceptions.UpstreamError` Class Reference

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

10.84.1 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 \(2493\)](#)

10.85 rpki.exceptions.WrongEContentType Class Reference

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

10.85.1 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 \(2493\)](#)

10.86 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](#)

10.86.1 Detailed Description

Definition at line 497 of file `https.py`.

10.86.2 Member Function Documentation

10.86.2.1 `def rpki.https.http_client.__init__ (self, queue, hostport, cert = None, key = None, ta = ())`

Definition at line 501 of file `https.py`.

10.86.2.2 `def rpki.https.http_client.handle_close (self)`

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

Definition at line 595 of file `https.py`.

10.86.2.3 `def rpki.https.http_client.handle_connect (self)`

Definition at line 523 of file `https.py`.

10.86.2.4 def rpki.https.http_client.handle_error (*self*)

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

Definition at line 610 of file https.py.

10.86.2.5 def rpki.https.http_client.handle_message (*self*)

Definition at line 566 of file https.py.

10.86.2.6 def rpki.https.http_client.handle_no_content_length (*self*)

Definition at line 555 of file https.py.

10.86.2.7 def rpki.https.http_client.handle_timeout (*self*)

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

Definition at line 604 of file https.py.

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

Definition at line 558 of file https.py.

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

Definition at line 551 of file https.py.

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

Definition at line 514 of file https.py.

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

Definition at line 541 of file https.py.

10.86.3 Member Data Documentation**10.86.3.1 rpki.https.http_client.cert**

Definition at line 509 of file https.py.

10.86.3.2 rpki.https.http_client.expect_close

Definition at line 508 of file https.py.

10.86.3.3 rpki.https.http_client.hostport

Definition at line 506 of file https.py.

10.86.3.4 rpki.https.http_client.key

Definition at line 510 of file https.py.

10.86.3.5 rpki.https.http_client.parse_type = http_response [static]

Definition at line 499 of file https.py.

10.86.3.6 rpki.https.http_client.queue

Definition at line 505 of file https.py.

10.86.3.7 rpki.https.http_client.retry_read

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

Definition at line 545 of file https.py.

10.86.3.8 rpki.https.http_client.retry_write

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

Definition at line 547 of file https.py.

10.86.3.9 rpki.https.http_client.state

Definition at line 507 of file https.py.

10.86.3.10 rpki.https.http_client.ta

Definition at line 511 of file https.py.

10.86.3.11 rpki.https.http_client.tls

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

Definition at line 527 of file https.py.

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

- [https.py \(2493\)](#)

10.87 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

10.87.1 Detailed Description

Definition at line 456 of file `https.py`.

10.87.2 Member Function Documentation

10.87.2.1 `def rpki.https.http_listener.__init__ (self, handlers, port = 80, host = "", cert = None, key = None, ta = None, dynamic_ta = None)`

Definition at line 460 of file `https.py`.

10.87.2.2 `def rpki.https.http_listener.handle_accept (self)`

Definition at line 480 of file `https.py`.

10.87.2.3 `def rpki.https.http_listener.handle_error (self)`

Definition at line 489 of file `https.py`.

10.87.3 Member Data Documentation

10.87.3.1 rpki.https.http_listener.cert

Definition at line 464 of file https.py.

10.87.3.2 rpki.https.http_listener.dynamic_ta

Definition at line 467 of file https.py.

10.87.3.3 rpki.https.http_listener.handlers

Definition at line 463 of file https.py.

10.87.3.4 rpki.https.http_listener.key

Definition at line 465 of file https.py.

10.87.3.5 rpki.https.http_listener.log = logger [static]

Definition at line 458 of file https.py.

10.87.3.6 rpki.https.http_listener.ta

Definition at line 466 of file https.py.

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

- [https.py \(2493\)](#)

10.88 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"

10.88.1 Detailed Description

Definition at line 63 of file `https.py`.

10.88.2 Member Function Documentation

10.88.2.1 `def rpki.https.http_message.__init__ (self, version = None, body = None, headers = None)`

Definition at line 67 of file `https.py`.

10.88.2.2 `def rpki.https.http_message.__str__ (self)`

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

10.88.2.3 def rpki.https.http_message.format (*self*)

Definition at line 103 of file https.py.

10.88.2.4 def rpki.https.http_message.normalize_headers (*self*, *headers* = None)

Definition at line 73 of file https.py.

10.88.2.5 def rpki.https.http_message.parse_from_wire (*cls*, *headers*)

Definition at line 92 of file https.py.

10.88.2.6 def rpki.https.http_message.parse_version (*self*, *version*)

Definition at line 118 of file https.py.

10.88.2.7 def rpki.https.http_message.persistent (*self*)

Definition at line 123 of file https.py.

10.88.3 Member Data Documentation**10.88.3.1 rpki.https.http_message.body**

Definition at line 69 of file https.py.

10.88.3.2 rpki.https.http_message.headers

Definition at line 70 of file https.py.

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

Definition at line 65 of file `https.py`.

10.88.3.4 `rpki.https.http_message.version`

Definition at line 68 of file `https.py`.

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

- [https.py \(2493\)](#)

10.89 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`

10.89.1 Detailed Description

Definition at line 619 of file https.py.

10.89.2 Member Function Documentation

10.89.2.1 `def rpki.https.http_queue.__init__ (self, hostport, cert = None, key = None, ta = ())`

Definition at line 623 of file https.py.

10.89.2.2 `def rpki.https.http_queue.detach (self, client)`

Definition at line 653 of file https.py.

10.89.2.3 `def rpki.https.http_queue.request (self, requests)`

Definition at line 633 of file https.py.

10.89.2.4 `def rpki.https.http_queue.restart (self)`

Definition at line 637 of file https.py.

10.89.2.5 `def rpki.https.http_queue.return_result (self, result)`

Definition at line 658 of file https.py.

10.89.2.6 `def rpki.https.http_queue.send_request (self)`

Definition at line 649 of file https.py.

10.89.3 Member Data Documentation

10.89.3.1 `rpki.https.http_queue.cert`

Definition at line 629 of file `https.py`.

10.89.3.2 `rpki.https.http_queue.client`

Definition at line 627 of file `https.py`.

10.89.3.3 `rpki.https.http_queue.hostport`

Definition at line 626 of file `https.py`.

10.89.3.4 `rpki.https.http_queue.key`

Definition at line 630 of file `https.py`.

10.89.3.5 `rpki.https.http_queue.log = logger` [static]

Definition at line 621 of file `https.py`.

10.89.3.6 `rpki.https.http_queue.queue`

Definition at line 628 of file `https.py`.

10.89.3.7 `rpki.https.http_queue.ta`

Definition at line 631 of file `https.py`.

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

- [https.py \(2493\)](#)

10.90 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](#)

10.90.1 Detailed Description

Definition at line 132 of file [https.py](#).

10.90.2 Member Function Documentation

10.90.2.1 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 134 of file [https.py](#).

10.90.2.2 def [rpki.https.http_request.format_first_line](#) (*self*)

Definition at line 149 of file [https.py](#).

10.90.2.3 def rpki.https.http_request.parse_first_line (self, cmd, path, version)

Definition at line 144 of file https.py.

10.90.3 Member Data Documentation

10.90.3.1 rpki.https.http_request.callback

Definition at line 140 of file https.py.

10.90.3.2 rpki.https.http_request.cmd

Definition at line 138 of file https.py.

10.90.3.3 rpki.https.http_request.errback

Definition at line 141 of file https.py.

10.90.3.4 rpki.https.http_request.path

Definition at line 139 of file https.py.

10.90.3.5 rpki.https.http_request.retried

Definition at line 142 of file https.py.

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

- [https.py \(2493\)](#)

10.91 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`

10.91.1 Detailed Description

Definition at line 153 of file https.py.

10.91.2 Member Function Documentation

10.91.2.1 `def rpki.https.http_response.__init__ (self, code = None, reason = None, version = default_http_version, body = None, headers)`

Definition at line 155 of file https.py.

10.91.2.2 `def rpki.https.http_response.format_first_line (self)`

Definition at line 165 of file https.py.

10.91.2.3 `def rpki.https.http_response.parse_first_line (self, version, code, reason)`

Definition at line 160 of file https.py.

10.91.3 Member Data Documentation

10.91.3.1 `rpki.https.http_response.code`

Definition at line 157 of file https.py.

10.91.3.2 rpki.https.http_response.reason

Definition at line 158 of file https.py.

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

- [https.py \(2493\)](#)

10.92 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](#)

10.92.1 Detailed Description

Definition at line 365 of file https.py.

10.92.2 Member Function Documentation

10.92.2.1 `def rpki.https.http_server.__init__ (self, conn, handlers, cert = None, key = None, ta = (), dynamic_ta = None)`

Definition at line 369 of file https.py.

10.92.2.2 `def rpki.https.http_server.find_handler (self, path)`

Helper method to search self.handlers.

Definition at line 404 of file https.py.

10.92.2.3 `def rpki.https.http_server.handle_message (self)`

Definition at line 413 of file https.py.

10.92.2.4 `def rpki.https.http_server.handle_no_content_length (self)`

Definition at line 401 of file https.py.

10.92.2.5 `def rpki.https.http_server.send_error (self, code, reason)`

Definition at line 436 of file https.py.

10.92.2.6 `def rpki.https.http_server.send_message (self, code, reason = "OK", body = None)`

Definition at line 442 of file https.py.

10.92.2.7 `def rpki.https.http_server.send_reply (self, code, body)`

Definition at line 439 of file https.py.

10.92.2.8 `def rpki.https.http_server.tls_accept (self)`

Definition at line 393 of file https.py.

10.92.3 Member Data Documentation**10.92.3.1** `rpki.https.http_server.expect_close`

Definition at line 373 of file https.py.

10.92.3.2 `rpki.https.http_server.handlers`

Definition at line 371 of file https.py.

10.92.3.3 `rpki.https.http_server.parse_type = http_request` [static]

Definition at line 367 of file https.py.

10.92.3.4 `rpki.https.http_server.retry_read`

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

Definition at line 397 of file https.py.

10.92.3.5 `rpki.https.http_server.retry_write`

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

Definition at line 399 of file `https.py`.

10.92.3.6 `rpki.https.http_server.tls`

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

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

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

- [https.py](#) (2493)

10.93 `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 `initate_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
- [timeout](#) = [default_timeout](#)
- [tls](#) = None

10.93.1 Detailed Description

Definition at line 174 of file https.py.

10.93.2 Member Function Documentation

10.93.2.1 `def rpki.https.http_stream.__init__ (self, conn = None)`

Definition at line 183 of file https.py.

10.93.2.2 `def rpki.https.http_stream.chunk_body (self)`

Definition at line 243 of file https.py.

10.93.2.3 `def rpki.https.http_stream.chunk_discard_crlf (self)`

Definition at line 250 of file https.py.

10.93.2.4 `def rpki.https.http_stream.chunk_discard_trailer (self)`

Definition at line 256 of file https.py.

10.93.2.5 def rpki.https.http_stream.chunk_header (self)

Definition at line 233 of file https.py.

10.93.2.6 def rpki.https.http_stream.close (self, force = False)

Definition at line 345 of file https.py.

10.93.2.7 def rpki.https.http_stream.collect_incoming_data (self, data)

Buffer the data

Definition at line 204 of file https.py.

10.93.2.8 def rpki.https.http_stream.found_terminator (self)

Definition at line 216 of file https.py.

10.93.2.9 def rpki.https.http_stream.get_buffer (self)

Definition at line 211 of file https.py.

10.93.2.10 def rpki.https.http_stream.handle_body (self)

Definition at line 263 of file https.py.

10.93.2.11 def rpki.https.http_stream.handle_close (self)

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

Definition at line 281 of file https.py.

10.93.2.12 def rpki.https.http_stream.handle_error (*self*)

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

Definition at line 267 of file https.py.

10.93.2.13 def rpki.https.http_stream.handle_read (*self*)

Definition at line 299 of file https.py.

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

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

Definition at line 277 of file https.py.

10.93.2.15 def rpki.https.http_stream.handle_write (*self*)

Definition at line 320 of file https.py.

10.93.2.16 def rpki.https.http_stream.initate_send (*self*)

Definition at line 330 of file https.py.

10.93.2.17 def rpki.https.http_stream.log_cert (*self*, *tag*, *x*)

Definition at line 361 of file https.py.

10.93.2.18 def rpki.https.http_stream.readable (*self*)

Definition at line 293 of file https.py.

10.93.2.19 def rpki.https.http_stream.recv (*self*, *buffer_size*)

Definition at line 289 of file https.py.

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

Definition at line 189 of file https.py.

10.93.2.21 def rpki.https.http_stream.send (*self*, *data*)

Definition at line 285 of file https.py.

10.93.2.22 def rpki.https.http_stream.update_timeout (*self*)

Definition at line 198 of file https.py.

10.93.2.23 def rpki.https.http_stream.writeable (*self*)

Definition at line 296 of file https.py.

10.93.3 Member Data Documentation**10.93.3.1 rpki.https.http_stream.buffer**

Definition at line 185 of file https.py.

10.93.3.2 rpki.https.http_stream.chunk_handler

Definition at line 191 of file https.py.

10.93.3.3 rpki.https.http_stream.log = logger [static]

Definition at line 176 of file https.py.

10.93.3.4 rpki.https.http_stream.msg

Definition at line 223 of file https.py.

10.93.3.5 rpki.https.http_stream.retry_read = None [static]

Reimplemented in [rpki.https.http_server](#), and [rpki.https.http_client](#).

Definition at line 178 of file https.py.

10.93.3.6 rpki.https.http_stream.retry_write = None [static]

Reimplemented in [rpki.https.http_server](#), and [rpki.https.http_client](#).

Definition at line 179 of file https.py.

10.93.3.7 rpki.https.http_stream.timeout = default_timeout [static]

Definition at line 181 of file https.py.

10.93.3.8 rpki.https.http_stream.timer

Definition at line 186 of file https.py.

10.93.3.9 rpki.https.http_stream.tls = None [static]

Reimplemented in [rpki.https.http_server](#), and [rpki.https.http_client](#).

Definition at line 177 of file https.py.

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

- [https.py \(2493\)](#)

10.94 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

10.94.1 Detailed Description

IPv4 address.

Derived from long, but supports IPv4 print syntax.

Definition at line 47 of file ipaddrs.py.

10.94.2 Member Function Documentation

10.94.2.1 def rpki.ipaddrs.v4addr.__new__ (cls, x)

Construct a v4addr object.

Definition at line 56 of file ipaddrs.py.

10.94.2.2 def rpki.ipaddrs.v4addr.__str__ (self)

Convert a v4addr object to string format.

Definition at line 74 of file ipaddrs.py.

10.94.2.3 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.

10.94.2.4 def rpki.ipaddrs.v4addr.to_bytes (self)

Convert a v4addr object to a raw byte string.

Definition at line 65 of file ipaddrs.py.

10.94.3 Member Data Documentation

10.94.3.1 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 \(2424\)](#)

10.95 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

10.95.1 Detailed Description

IPv6 address.

Derived from long, but supports IPv6 print syntax.

Definition at line 78 of file ipaddrs.py.

10.95.2 Member Function Documentation

10.95.2.1 def rpki.ipaddrs.v6addr.__new__ (cls, x)

Construct a v6addr object.

Definition at line 87 of file ipaddrs.py.

10.95.2.2 def rpki.ipaddrs.v6addr.__str__ (self)

Convert a v6addr object to string format.

Definition at line 104 of file ipaddrs.py.

10.95.2.3 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.

10.95.2.4 def rpki.ipaddrs.v6addr.to_bytes (self)

Convert a v6addr object to a raw byte string.

Definition at line 94 of file ipaddrs.py.

10.95.3 Member Data Documentation

10.95.3.1 `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 \(2424\)](#)

10.96 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](#)

10.96.1 Detailed Description

<bsc/> (Business Signing Context) element.

Definition at line 414 of file left_right.py.

10.96.2 Member Function Documentation

10.96.2.1 def rpki.left_right.bsc_elt.children (*self*)

Fetch all child objects that link to this BSC object.

Definition at line 445 of file left_right.py.

10.96.2.2 def rpki.left_right.bsc_elt.parents (*self*)

Fetch all parent objects that link to this BSC object.

Definition at line 441 of file left_right.py.

10.96.2.3 def rpki.left_right.bsc_elt.repositories (*self*)

Fetch all repository objects that link to this BSC object.

Definition at line 437 of file left_right.py.

10.96.2.4 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 449 of file left_right.py.

10.96.3 Member Data Documentation

10.96.3.1 `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 420 of file left_right.py.

10.96.3.2 `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 422 of file left_right.py.

10.96.3.3 `string rpki.left_right.bsc_elt.element_name = "bsc"` [static]

Definition at line 419 of file left_right.py.

10.96.3.4 `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 421 of file left_right.py.

10.96.3.5 `tuple rpki.left_right.bsc_elt.handles = (("self", self_elt),)` [static]

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

Definition at line 430 of file left_right.py.

10.96.3.6 rpki.left_right.bsc_elt.pkcs10_request = None [static]

Definition at line 433 of file left_right.py.

10.96.3.7 rpki.left_right.bsc_elt.private_key_id = None [static]

Definition at line 432 of file left_right.py.

10.96.3.8 rpki.left_right.bsc_elt.signing_cert = None [static]

Reimplemented in [irbe_cli.bsc_elt](#).

Definition at line 434 of file left_right.py.

10.96.3.9 rpki.left_right.bsc_elt.signing_cert_crl = None [static]

Reimplemented in [irbe_cli.bsc_elt](#).

Definition at line 435 of file left_right.py.

10.96.3.10 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 424 of file left_right.py.

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

- [left_right.py](#) (2504)

10.97 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_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](#)

10.97.1 Detailed Description

<child/> element.

Definition at line 632 of file left_right.py.

10.97.2 Member Function Documentation

10.97.2.1 `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 661 of file left_right.py.

10.97.2.2 `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 653 of file left_right.py.

10.97.2.3 `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 685 of file left_right.py.

10.97.2.4 `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 657 of file left_right.py.

10.97.2.5 `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 675 of file left_right.py.

10.97.2.6 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 695 of file left_right.py.

10.97.3 Member Data Documentation

10.97.3.1 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 638 of file left_right.py.

10.97.3.2 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 640 of file left_right.py.

10.97.3.3 rpki.left_right.child_elt.bpkcert = None [static]

Definition at line 649 of file left_right.py.

10.97.3.4 rpki.left_right.child_elt.bpkglue = None [static]

Definition at line 650 of file left_right.py.

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

Definition at line 651 of file left_right.py.

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

Definition at line 637 of file left_right.py.

10.97.3.7 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 639 of file left_right.py.

10.97.3.8 tuple rpki.left_right.child_elt.handles = ("self", self_elt), ("bsc", bsc_elt)) [static]

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

Definition at line 647 of file left_right.py.

10.97.3.9 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 642 of file left_right.py.

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

- [left_right.py \(2504\)](#)

10.98 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](#)

10.98.1 Detailed Description

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

Definition at line 1127 of file [left_right.py](#).

10.98.2 Member Data Documentation

10.98.2.1 string [rpki.left_right.cms_msg.encoding](#) = "us-ascii" [static]

Definition at line 1132 of file [left_right.py](#).

10.98.2.2 [rpki.left_right.cms_msg.saxify](#) = [sax_handler.saxify](#) [static]

Reimplemented in [irbe_cli.left_right_cms_msg](#).

Definition at line 1134 of file [left_right.py](#).

10.98.2.3 [rpki.left_right.cms_msg.schema](#) = [rpki.relaxng.left_right](#) [static]

Definition at line 1133 of file [left_right.py](#).

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

- [left_right.py \(2504\)](#)

10.99 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](#), [rpki.left_right.route_origin_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](#)
- def [unimplemented_control](#)

Static Public Attributes

- tuple [handles](#) = ()
- [self_id](#) = None

10.99.1 Detailed Description

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

Definition at line 51 of file [left_right.py](#).

10.99.2 Member Function Documentation

10.99.2.1 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](#).

10.99.2.2 def rpki.left_right.data_elt.make_reply_clone_hook (self, r_pdu)

Set self_handle when cloning.

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

Definition at line 68 of file left_right.py.

10.99.2.3 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.

10.99.2.4 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 88 of file left_right.py.

10.99.2.5 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 73 of file left_right.py.

10.99.2.6 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 79 of file `left_right.py`.

10.99.2.7 `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.

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

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

Definition at line 95 of file `left_right.py`.

10.99.2.8 `def rpki.left_right.data_elt.unimplemented_control (self, controls)`

Uniform handling for unimplemented control operations.

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

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

10.99.3 Member Data Documentation

10.99.3.1 `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](#), [rpki.left_right.child_elt](#), and [rpki.left_right.route_origin_elt](#).

Definition at line 56 of file `left_right.py`.

10.99.3.2 `rpki.left_right.data_elt.self_id = None` [static]

Definition at line 58 of file left_right.py.

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

- [left_right.py \(2504\)](#)

10.100 rpki.left_right.left_right_namespace Class Reference

Inherits [object](#).

Inherited by [rpki.left_right.data_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/"

10.100.1 Detailed Description

XML namespace parameters for left-right protocol.

Definition at line 43 of file left_right.py.

10.100.2 Member Data Documentation

10.100.2.1 dictionary [rpki.left_right.left_right_namespace.nsmap](#) = { None : [xmlns](#) } [static]

Definition at line 49 of file left_right.py.

10.100.2.2 string [rpki.left_right.left_right_namespace.xmlns](#) = "http://www.hactrn.net/uris/rpki/left-right-spec/" [static]

Definition at line 48 of file left_right.py.

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

- [left_right.py \(2504\)](#)

10.101 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

10.101.1 Detailed Description

<list_resources/> element.

Definition at line 1001 of file left_right.py.

10.101.2 Member Function Documentation

10.101.2.1 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 1010 of file left_right.py.

10.101.2.2 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 1026 of file left_right.py.

10.101.3 Member Data Documentation**10.101.3.1 rpki.left_right.list_resources_elt.asn**

Definition at line 1020 of file left_right.py.

```
10.101.3.2 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 1007 of file left_right.py.

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

Definition at line 1006 of file left_right.py.

10.101.3.4 rpki.left_right.list_resources_elt.ipv4

Definition at line 1022 of file left_right.py.

10.101.3.5 rpki.left_right.list_resources_elt.ipv6

Definition at line 1024 of file left_right.py.

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

Definition at line 1008 of file left_right.py.

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

- [left_right.py \(2504\)](#)

10.102 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"

10.102.1 Detailed Description

<list_roa_requests/> element.

Definition at line 1036 of file left_right.py.

10.102.2 Member Function Documentation

10.102.2.1 `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 1044 of file left_right.py.

10.102.3 Member Data Documentation

10.102.3.1 `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 1042 of file left_right.py.

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

Definition at line 1041 of file left_right.py.

10.102.3.3 `rpki.left_right.list_roa_requests_elt.ipv4`

Definition at line 1052 of file left_right.py.

10.102.3.4 `rpki.left_right.list_roa_requests_elt.ipv6`

Definition at line 1054 of file left_right.py.

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

- [left_right.py](#) (2504)

10.103 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.

10.103.1 Detailed Description

Left-right PDU.

Definition at line 1075 of file [left_right.py](#).

10.103.2 Member Function Documentation

10.103.2.1 def rpki.left_right.msg.serve_top_level (self, gctx, cb)

Serve one msg PDU.

Definition at line 1091 of file [left_right.py](#).

10.103.3 Member Data Documentation

10.103.3.1 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, route_origin_elt, list_resources_elt,
                list_roa_requests_elt, report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented in [irbe_cli.left_right_msg](#).

Definition at line 1086 of file left_right.py.

10.103.3.2 rpki::left_right.msg::version = 1 [static]

Protocol version.

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

Definition at line 1082 of file left_right.py.

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

- [left_right.py \(2504\)](#)

10.104 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](#)

Static Public Attributes

- tuple [attributes](#)
XML attributes for this element.

- tuple `booleans` = ("rekey", "reissue", "revoke")
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`

10.104.1 Detailed Description

`<parent/> element.`

Definition at line 532 of file `left_right.py`.

10.104.2 Member Function Documentation

10.104.2.1 `def rpki.left_right.parent_elt.cas (self)`

Fetch all CA objects that link to this parent object.

Definition at line 559 of file `left_right.py`.

10.104.2.2 `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 595 of file `left_right.py`.

10.104.2.3 def rpki.left_right.parent_elt.repository (self)

Fetch repository object to which this parent object links.

Definition at line 555 of file left_right.py.

10.104.2.4 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 563 of file left_right.py.

10.104.2.5 def rpki.left_right.parent_elt.serve_rekey (self, cb, eb)

Handle a left-right rekey action for this parent.

Definition at line 575 of file left_right.py.

10.104.2.6 def rpki.left_right.parent_elt.serve_revoke (self, cb, eb)

Handle a left-right revoke action for this parent.

Definition at line 585 of file left_right.py.

10.104.3 Member Data Documentation**10.104.3.1 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 538 of file left_right.py.

10.104.3.2 `tuple rpki.left_right.parent_elt.booleans = ("rekey", "reissue",
 "revoke") [static]`

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

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

Definition at line 541 of file left_right.py.

10.104.3.3 `rpki.left_right.parent_elt.bpki_cms_cert = None [static]`

Definition at line 550 of file left_right.py.

10.104.3.4 `rpki.left_right.parent_elt.bpki_cms_glue = None [static]`

Definition at line 551 of file left_right.py.

10.104.3.5 `rpki.left_right.parent_elt.bpki_https_cert = None [static]`

Definition at line 552 of file left_right.py.

10.104.3.6 `rpki.left_right.parent_elt.bpki_https_glue = None [static]`

Definition at line 553 of file left_right.py.

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

Definition at line 537 of file left_right.py.

10.104.3.8 `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 540 of file left_right.py.

10.104.3.9 `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 548 of file left_right.py.

10.104.3.10 `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_https_glue", rpki.x509.X509),
                  "peer_contact_uri", "sia_base", "sender_name", "recipient_name")
```

Definition at line 543 of file left_right.py.

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

- [left_right.py \(2504\)](#)

10.105 rpki.left_right.report_error_elt Class Reference

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

Public Member Functions

- def [from_exception](#)

Public Attributes

- [error_code](#)
- [self_handle](#)
- [text](#)

Static Public Attributes

- tuple [attributes](#) = ("tag", "self_handle", "error_code")
XML attributes for this element.
- string [element_name](#) = "report_error"

10.105.1 Detailed Description

<report_error/> element.

Definition at line 1056 of file left_right.py.

10.105.2 Member Function Documentation

10.105.2.1 def rpki.left_right.report_error_elt.from_exception (*cls*, *e*, *self_handle* = None)

Generate a <report_error/> element from an exception.

Definition at line 1065 of file left_right.py.

10.105.3 Member Data Documentation

10.105.3.1 `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 1062 of file `left_right.py`.

10.105.3.2 `string rpki.left_right.report_error_elt.element_name = "report_error" [static]`

Definition at line 1061 of file `left_right.py`.

10.105.3.3 `rpki.left_right.report_error_elt.error_code`

Definition at line 1071 of file `left_right.py`.

10.105.3.4 `rpki.left_right.report_error_elt.self_handle`

Definition at line 1070 of file `left_right.py`.

10.105.3.5 `rpki.left_right.report_error_elt.text`

Definition at line 1072 of file `left_right.py`.

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

- [left_right.py \(2504\)](#)

10.106 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_cms_cert](#) = None
- [bpki_cms_glue](#) = None
- [bpki_https_cert](#) = None
- [bpki_https_glue](#) = None
- string [element_name](#) = "repository"
- 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))
- tuple [sql_template](#)

10.106.1 Detailed Description

<repository/> element.

Definition at line 461 of file left_right.py.

10.106.2 Member Function Documentation

10.106.2.1 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 485 of file left_right.py.

10.106.2.2 def rpki.left_right.repository_elt.parents (*self*)

Fetch all parent objects that link to this repository object.

Definition at line 481 of file left_right.py.

10.106.2.3 def rpki.left_right.repository_elt.publish (*self*, *obj*, *uri*, *callback*, *errback*)

Publish one object in the repository.

Definition at line 516 of file left_right.py.

10.106.2.4 def rpki.left_right.repository_elt.withdraw (*self*, *obj*, *uri*, *callback*, *errback*)

Withdraw one object from the repository.

Definition at line 524 of file left_right.py.

10.106.3 Member Data Documentation**10.106.3.1 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 467 of file left_right.py.

10.106.3.2 rpki.left_right.repository_elt.bpki_cms_cert = None [static]

Definition at line 476 of file left_right.py.

10.106.3.3 `rpki.left_right.repository_elt.bpki_cms_glue = None` `[static]`

Definition at line 477 of file left_right.py.

10.106.3.4 `rpki.left_right.repository_elt.bpki_https_cert = None` `[static]`

Definition at line 478 of file left_right.py.

10.106.3.5 `rpki.left_right.repository_elt.bpki_https_glue = None` `[static]`

Definition at line 479 of file left_right.py.

10.106.3.6 `string rpki.left_right.repository_elt.element_name = "repository"`
`[static]`

Definition at line 466 of file left_right.py.

10.106.3.7 `tuple rpki.left_right.repository_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 468 of file left_right.py.

10.106.3.8 `tuple rpki.left_right.repository_elt.handles = (("self", self_elt),
("bsc", bsc_elt))` `[static]`

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

Definition at line 474 of file left_right.py.

10.106.3.9 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_cms_cert", rpki.x509.X509), ("bpki_cms_glue", rpki.x509.X509),  
                  ("bpki_https_cert", rpki.x509.X509), ("bpki_https_glue", rpki.x509.X509))
```

Definition at line 470 of file left_right.py.

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

- [left_right.py \(2504\)](#)

10.107 rpki.left_right.route_origin_elt Class Reference

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

Inherited by [irbe_cli.route_origin_elt](#).

Public Member Functions

- def [ca_detail](#)
- def [ee_uri](#)
- def [ee_uri_tail](#)
- def [generate_roa](#)
- def [regenerate_roa](#)
- def [roa_uri](#)
- def [roa_uri_tail](#)
- def [serve_post_save_hook](#)
- def [sql_delete_hook](#)
- def [sql_fetch_hook](#)
- def [sql_insert_hook](#)
- def [startElement](#)
- def [update_roa](#)
- def [withdraw_roa](#)

Public Attributes

- [as_number](#)
- [ipv4](#)
- [ipv6](#)

Static Public Attributes

- tuple `attributes` = ("action", "tag", "self_handle", "route_origin_handle", "as_number", "ipv4", "ipv6")

XML attributes for this element.

- tuple `booleans` = ("suppress_publication",)

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

- `ca_detail_id` = None
- `cert` = None
- string `element_name` = "route_origin"
- tuple `handles` = (("self", self_elt),)
- `publish_ee_separately` = False

Whether to publish the ROA EE certificate separately from the ROA.

- `roa` = None
- tuple `sql_template`

10.107.1 Detailed Description

<route_origin/> element.

Definition at line 732 of file left_right.py.

10.107.2 Member Function Documentation

10.107.2.1 def rpki.left_right.route_origin_elt.ca_detail (self)

Fetch all `ca_detail` objects that link to this `route_origin` object.

Definition at line 791 of file left_right.py.

10.107.2.2 def rpki.left_right.route_origin_elt.aa_uri (self, ca)

Return the publication URI for this `route_origin`'s ROA's EE certificate.

Definition at line 997 of file left_right.py.

10.107.2.3 def rpki.left_right.route_origin_elt.ee_uri_tail (self)

Return the tail (filename) portion of the URI for this route_origin's ROA's EE certificate.

Definition at line 993 of file left_right.py.

10.107.2.4 def rpki.left_right.route_origin_elt.generate_roa (self, callback, errback)

Generate a ROA based on this <route_origin/> object.

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 859 of file left_right.py.

10.107.2.5 def rpki.left_right.route_origin_elt.regenerate_roa (self, callback, errback)

Reissue ROA associated with this route_origin.

Definition at line 976 of file left_right.py.

10.107.2.6 def rpki.left_right.route_origin_elt.roa_uri (self, ca, key = None)

Return the publication URI for this route_origin's ROA.

Definition at line 985 of file left_right.py.

10.107.2.7 `def rpki.left_right.route_origin_elt.roa_uri_tail (self, key = None)`

Return the tail (filename portion) of the publication URI for this route_origin's ROA.

Definition at line 989 of file left_right.py.

10.107.2.8 `def rpki.left_right.route_origin_elt.serve_post_save_hook (self, q_pdu, r_pdu, cb, eb)`

Extra server actions for route_origin_elt.

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

Definition at line 795 of file left_right.py.

10.107.2.9 `def rpki.left_right.route_origin_elt.sql_delete_hook (self)`

Extra SQL delete actions for route_origin_elt -- handle address ranges.

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 784 of file left_right.py.

10.107.2.10 `def rpki.left_right.route_origin_elt.sql_fetch_hook (self)`

Extra SQL fetch actions for route_origin_elt -- handle prefix list.

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 755 of file left_right.py.

10.107.2.11 `def rpki.left_right.route_origin_elt.sql_insert_hook (self)`

Extra SQL insert actions for route_origin_elt -- handle address ranges.

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 769 of file left_right.py.

10.107.2.12 **def rpki.left_right.route_origin_elt.startElement (self, stack, name, attrs)**

Handle <route_origin/> element. This requires special processing due to the data types of some of the attributes.

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

Definition at line 802 of file left_right.py.

10.107.2.13 **def rpki.left_right.route_origin_elt.update_roa (self, callback)**

Bring this route_origin's ROA up to date if necessary.

Definition at line 816 of file left_right.py.

10.107.2.14 **def rpki.left_right.route_origin_elt.withdraw_roa (self, callback, errback, regenerate = False)**

Withdraw ROA associated with this route_origin.

In order to preserve make-before-break properties without duplicating code, this method also handles generating a replacement ROA when requested.

Definition at line 934 of file left_right.py.

10.107.3 Member Data Documentation

10.107.3.1 **rpki.left_right.route_origin_elt.as_number**

Reimplemented in [irbe_cli.route_origin_elt](#).

Definition at line 810 of file left_right.py.

```
10.107.3.2 tuple rpki.left_right.route_origin_elt.attributes = ("action", "tag",  
    "self_handle", "route_origin_handle", "as_number", "ipv4",  
    "ipv6") [static]
```

XML attributes for this element.

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

Definition at line 738 of file left_right.py.

```
10.107.3.3 tuple rpki.left_right.route_origin_elt.booleans =  
    ("suppress_publication",) [static]
```

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

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

Definition at line 739 of file left_right.py.

```
10.107.3.4 rpki.left_right.route_origin_elt.ca_detail_id = None [static]
```

Definition at line 747 of file left_right.py.

```
10.107.3.5 rpki.left_right.route_origin_elt.cert = None [static]
```

Definition at line 748 of file left_right.py.

```
10.107.3.6 string rpki.left_right.route_origin_elt.element_name =  
    "route_origin" [static]
```

Definition at line 737 of file left_right.py.

10.107.3.7 `tuple rpki.left_right.route_origin_elt.handles = (('self', self_elt),)`
[static]

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

Definition at line 745 of file left_right.py.

10.107.3.8 `rpki.left_right.route_origin_elt.ipv4`

Reimplemented in [irbe_cli.route_origin_elt](#).

Definition at line 812 of file left_right.py.

10.107.3.9 `rpki.left_right.route_origin_elt.ipv6`

Reimplemented in [irbe_cli.route_origin_elt](#).

Definition at line 814 of file left_right.py.

10.107.3.10 `rpki::left_right.route_origin_elt::publish_ee_separately = False`
[static]

Whether to publish the ROA EE certificate separately from the ROA.

Definition at line 753 of file left_right.py.

10.107.3.11 `rpki.left_right.route_origin_elt.roa = None` [static]

Definition at line 749 of file left_right.py.

10.107.3.12 `tuple rpki.left_right.route_origin_elt.sql_template` [static]

Initial value:

```
rpki.sql.template("route_origin", "route_origin_id", "route_origin_handle",
```

```
"ca_detail_id", "self_id", "as_number",  
("roa", rpki.x509.ROA),  
("cert", rpki.x509.X509))
```

Definition at line 741 of file left_right.py.

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

- [left_right.py \(2504\)](#)

10.108 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"

10.108.1 Detailed Description

SAX handler for Left-Right protocol.

Definition at line 1118 of file left_right.py.

10.108.2 Member Data Documentation

10.108.2.1 string rpki.left_right.sax_handler.name = "msg" [static]

Definition at line 1124 of file left_right.py.

10.108.2.2 rpki.left_right.sax_handler.pdu = msg [static]

Reimplemented in [irbe_cli.left_right_sax_handler](#).

Definition at line 1123 of file left_right.py.

10.108.2.3 string rpki.left_right.sax_handler.version = "1" [static]

Definition at line 1125 of file left_right.py.

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

- [left_right.py \(2504\)](#)

10.109 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 [parents](#)
- def [regenerate_crls_and_manifests](#)
- def [repositories](#)
- def [route_origins](#)
- def [serve_fetch_all](#)
- def [serve_fetch_handle](#)
- def [serve_fetch_one_maybe](#)
- def [serve_post_save_hook](#)
- def [serve_rekey](#)
- def [serve_revoke](#)
- 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")

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

10.109.1 Detailed Description

`<self/> element.`

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

10.109.2 Member Function Documentation

10.109.2.1 `def rpki.left_right.self_elt.bscs (self)`

Fetch all BSC objects that link to this self object.

Definition at line 140 of file `left_right.py`.

10.109.2.2 `def rpki.left_right.self_elt.children (self)`

Fetch all child objects that link to this self object.

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

10.109.2.3 `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 217 of file `left_right.py`.

10.109.2.4 def rpki.left_right.self_elt.parents (*self*)

Fetch all parent objects that link to this self object.

Definition at line 148 of file left_right.py.

10.109.2.5 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 352 of file left_right.py.

10.109.2.6 def rpki.left_right.self_elt.repositories (*self*)

Fetch all repository objects that link to this self object.

Definition at line 144 of file left_right.py.

10.109.2.7 def rpki.left_right.self_elt.route_origins (*self*)

Fetch all route_origin objects that link to this self object.

Definition at line 156 of file left_right.py.

10.109.2.8 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 209 of file left_right.py.

10.109.2.9 **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 203 of file left_right.py.

10.109.2.10 **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 195 of file left_right.py.

10.109.2.11 **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 160 of file left_right.py.

10.109.2.12 **def rpki.left_right.self_elt.serve_rekey (self, cb, eb)**

Handle a left-right rekey action for this self.

Definition at line 173 of file left_right.py.

10.109.2.13 def rpki.left_right.self_elt.serve_revoke (self, cb, eb)

Handle a left-right revoke action for this self.

Definition at line 184 of file left_right.py.

10.109.2.14 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 270 of file left_right.py.

10.109.2.15 def rpki.left_right.self_elt.update_roas (self, cb)

Generate or update ROAs for this self's route_origin objects.

Definition at line 403 of file left_right.py.

10.109.3 Member Data Documentation

10.109.3.1 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 125 of file left_right.py.

10.109.3.2 `tuple rpki.left_right.self_elt.booleans = ("rekey", "reissue", "revoke", "run_now", "publish_world_now") [static]`

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

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

Definition at line 127 of file left_right.py.

10.109.3.3 `rpki.left_right.self_elt.bpki_cert = None [static]`

Definition at line 137 of file left_right.py.

10.109.3.4 `rpki.left_right.self_elt.bpki_glue = None [static]`

Definition at line 138 of file left_right.py.

10.109.3.5 `rpki.left_right.self_elt.crl_interval = None [static]`

Definition at line 135 of file left_right.py.

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

Definition at line 124 of file left_right.py.

10.109.3.7 `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 126 of file left_right.py.

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

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

Definition at line 132 of file left_right.py.

10.109.3.9 rpki.left_right.self_elt.regen_margin = None [static]

Definition at line 136 of file left_right.py.

10.109.3.10 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", rpki.x509.X509))
```

Definition at line 129 of file left_right.py.

10.109.3.11 rpki.left_right.self_elt.use_hsm = False [static]

Definition at line 134 of file left_right.py.

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

- [left_right.py \(2504\)](#)

10.110 rpki.log.logger Class Reference

Inherits [object](#).

Public Member Functions

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

Public Attributes

- [priority](#)

10.110.1 Detailed Description

Closure for logging.

Definition at line 70 of file log.py.

10.110.2 Member Function Documentation

10.110.2.1 def rpki.log.logger.__call__ (*self*, *message*)

Definition at line 78 of file log.py.

10.110.2.2 def rpki.log.logger.__init__ (*self*, *priority*)

Definition at line 75 of file log.py.

10.110.3 Member Data Documentation

10.110.3.1 rpki.log.logger.priority

Definition at line 76 of file log.py.

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

- [log.py \(2452\)](#)

10.111 rpki.manifest.FileAndHash Class Reference

Inherits [Sequence](#).

Public Member Functions

- def [__init__](#)

Public Attributes

- [file](#)
- [hash](#)

10.111.1 Detailed Description

Definition at line 27 of file manifest.py.

10.111.2 Member Function Documentation

10.111.2.1 `def rpki.manifest.FileAndHash.__init__ (self, optional = 0, default = "")`

Definition at line 28 of file manifest.py.

10.111.3 Member Data Documentation

10.111.3.1 rpki.manifest.FileAndHash.file

Definition at line 29 of file manifest.py.

10.111.3.2 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 \(2424\)](#)

10.112 rpki.manifest.FilesAndHashes Class Reference

Inherits [SequenceOf](#).

Public Member Functions

- `def __init__`

10.112.1 Detailed Description

Definition at line 34 of file manifest.py.

10.112.2 Member Function Documentation

10.112.2.1 `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 \(2424\)](#)

10.113 rpki.manifest.Manifest Class Reference

Inherits [Sequence](#).

Public Member Functions

- `def __init__`

Public Attributes

- [explicitVersion](#)
- [fileHashAlg](#)
- [fileList](#)
- [manifestNumber](#)
- [nextUpdate](#)
- [thisUpdate](#)
- [version](#)

10.113.1 Detailed Description

Definition at line 38 of file manifest.py.

10.113.2 Member Function Documentation

10.113.2.1 `def rpki.manifest.Manifest.__init__ (self, optional = 0, default = "")`

Definition at line 39 of file manifest.py.

10.113.3 Member Data Documentation

10.113.3.1 `rpki.manifest.Manifest.explicitVersion`

Definition at line 41 of file manifest.py.

10.113.3.2 `rpki.manifest.Manifest.fileHashAlg`

Definition at line 45 of file manifest.py.

10.113.3.3 `rpki.manifest.Manifest.fileList`

Definition at line 46 of file manifest.py.

10.113.3.4 `rpki.manifest.Manifest.manifestNumber`

Definition at line 42 of file manifest.py.

10.113.3.5 `rpki.manifest.Manifest.nextUpdate`

Definition at line 44 of file manifest.py.

10.113.3.6 `rpki.manifest.Manifest.thisUpdate`

Definition at line 43 of file manifest.py.

10.113.3.7 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 \(2424\)](#)

10.114 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](#)

10.114.1 Detailed Description

<certificate/> element.

Definition at line 245 of file publication.py.

10.114.2 Member Data Documentation

10.114.2.1 string rpki.publication.certificate_elt.element_name = "certificate" [static]

Definition at line 250 of file publication.py.

10.114.2.2 rpki.publication.certificate_elt.payload_type = rpki.x509.X509 [static]

Definition at line 251 of file publication.py.

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

- [publication.py \(2493\)](#)

10.115 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](#)))

10.115.1 Detailed Description

<client/> element.

Definition at line 113 of file publication.py.

10.115.2 Member Function Documentation

10.115.2.1 def rpki.publication.client_elt.check_allowed_uri (self, uri)

Definition at line 160 of file publication.py.

10.115.2.2 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.

10.115.2.3 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.

10.115.2.4 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.

10.115.2.5 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.

10.115.3 Member Data Documentation

10.115.3.1 `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`.

10.115.3.2 `rpki.publication.client_elt.base_uri = None [static]`

Definition at line 124 of file `publication.py`.

10.115.3.3 `rpki.publication.client_elt.bpki_cert = None [static]`

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

10.115.3.4 `rpki.publication.client_elt.bpki_glue = None [static]`

Definition at line 126 of file `publication.py`.

10.115.3.5 `rpki.publication.client_elt.clear_https_ta_cache = False [static]`

Definition at line 128 of file `publication.py`.

10.115.3.6 `string rpki.publication.client_elt.element_name = "client" [static]`

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

10.115.3.7 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.

10.115.3.8 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](#) (2493)

10.116 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](#)

10.116.1 Detailed Description

Class to hold a CMS-signed publication PDU.

Definition at line 352 of file publication.py.

10.116.2 Member Data Documentation

10.116.2.1 string rpki.publication.cms_msg.encoding = "us-ascii" [static]

Definition at line 357 of file publication.py.

10.116.2.2 rpki.publication.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented in [irbe_cli.publication_cms_msg](#).

Definition at line 359 of file publication.py.

10.116.2.3 rpki.publication.cms_msg.schema = rpki.relaxng.publication [static]

Definition at line 358 of file publication.py.

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

- [publication.py](#) (2493)

10.117 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

10.117.1 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`.

10.117.2 Member Function Documentation

10.117.2.1 `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`.

10.117.2.2 `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`.

10.117.2.3 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.

10.117.2.4 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.

10.117.3 Member Data Documentation**10.117.3.1 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.

10.117.3.2 rpki.publication.config_elt.config_id

Definition at line 86 of file publication.py.

**10.117.3.3 string rpki.publication.config_elt.element_name = "config"
[static]**

Definition at line 73 of file publication.py.

10.117.3.4 `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`.

10.117.3.5 `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`.

10.117.3.6 `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](#) (2493)

10.118 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](#)

10.118.1 Detailed Description

Virtual class for control channel objects.

Definition at line 47 of file `publication.py`.

10.118.2 Member Function Documentation

10.118.2.1 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](#) (2493)

10.119 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](#)

10.119.1 Detailed Description

<crl/> element.

Definition at line 253 of file publication.py.

10.119.2 Member Data Documentation

10.119.2.1 string rpki.publication.crl_elt.element_name = "crl" [static]

Definition at line 258 of file publication.py.

10.119.2.2 rpki.publication.crl_elt.payload_type = rpki.x509.CRL [static]

Definition at line 259 of file publication.py.

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

- [publication.py \(2493\)](#)

10.120 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](#)

10.120.1 Detailed Description

<manifest/> element.

Definition at line 261 of file publication.py.

10.120.2 Member Data Documentation

10.120.2.1 string rpki.publication.manifest_elt.element_name = "manifest" [static]

Definition at line 266 of file publication.py.

10.120.2.2 rpki.publication.manifest_elt.payload_type = rpki.x509.SignedManifest [static]

Definition at line 267 of file publication.py.

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

- [publication.py \(2493\)](#)

10.121 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.

10.121.1 Detailed Description

Publication PDU.

Definition at line 299 of file publication.py.

10.121.2 Member Function Documentation

10.121.2.1 def rpki.publication.msg.serve_top_level (self, gctx, client, cb)

Serve one msg PDU.

Definition at line 313 of file publication.py.

10.121.3 Member Data Documentation

10.121.3.1 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, rep
```

Dispatch table of PDUs for this protocol.

Reimplemented in [irbe_cli.publication_msg](#).

Definition at line 310 of file publication.py.

10.121.3.2 rpki::publication.msg::version = 1 [static]

Protocol version.

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

Definition at line 306 of file publication.py.

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

- [publication.py \(2493\)](#)

10.122 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/"

10.122.1 Detailed Description

XML namespace parameters for publication protocol.

Definition at line 39 of file publication.py.

10.122.2 Member Data Documentation

10.122.2.1 dictionary [rpki.publication.publication_namespace.nsmap](#) = { None : [xmlns](#) } [static]

Definition at line 45 of file publication.py.

```
10.122.2.2 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 \(2493\)](#)

10.123 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 [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

10.123.1 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.

10.123.2 Member Function Documentation

10.123.2.1 **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 177 of file publication.py.

10.123.2.2 **def rpki.publication.publication_object_elt.serve_dispatch (*self*, *r_msg*, *cb*, *eb*)**

Action dispatch handler.

Definition at line 195 of file publication.py.

10.123.2.3 **def rpki.publication.publication_object_elt.serve_publish (*self*)**

Publish an object.

Definition at line 214 of file publication.py.

10.123.2.4 **def rpki.publication.publication_object_elt.serve_withdraw (*self*)**

Withdraw an object.

Definition at line 227 of file publication.py.

10.123.2.5 **def rpki.publication.publication_object_elt.toXML (*self*)**

Generate XML element for publishable object.

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

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

10.123.2.6 `def rpki.publication.publication_object_elt.uri_to_filename (self)`

Convert a URI to a local filename.

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

10.123.3 Member Data Documentation

10.123.3.1 `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`.

10.123.3.2 `rpki.publication.publication_object_elt.payload = None [static]`

Definition at line 175 of file `publication.py`.

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

- [publication.py](#) (2493)

10.124 `rpki.publication.report_error_elt` Class Reference

Inherits [rpki.xml_utils.base_elt](#), and [rpki.publication.publication_namespace](#).

Public Member Functions

- `def from_exception`

Public Attributes

- [error_code](#)

Static Public Attributes

- tuple [attributes](#) = ("tag", "[error_code](#)")
XML attributes for this element.
- string [element_name](#) = "report_error"

10.124.1 Detailed Description

`<report_error/>` element.

Definition at line 282 of file publication.py.

10.124.2 Member Function Documentation

10.124.2.1 `def rpki.publication.report_error_elt.from_exception (cls, exc)`

Generate a `<report_error/>` element from an exception.

Definition at line 291 of file publication.py.

10.124.3 Member Data Documentation

10.124.3.1 `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 288 of file publication.py.

10.124.3.2 `string rpki.publication.report_error_elt.element_name = "report_error" [static]`

Definition at line 287 of file publication.py.

10.124.3.3 rpki.publication.report_error_elt.error_code

Definition at line 296 of file publication.py.

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

- [publication.py \(2493\)](#)

10.125 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](#)

10.125.1 Detailed Description

```
<roa/> element.
```

Definition at line 269 of file publication.py.

10.125.2 Member Data Documentation

10.125.2.1 string rpki.publication.roa_elt.element_name = "roa" [static]

Definition at line 274 of file publication.py.

10.125.2.2 rpki.publication.roa_elt.payload_type = rpki.x509.ROA [static]

Definition at line 275 of file publication.py.

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

- [publication.py \(2493\)](#)

10.126 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"

10.126.1 Detailed Description

SAX handler for publication protocol.

Definition at line 343 of file `publication.py`.

10.126.2 Member Data Documentation

10.126.2.1 string `rpki.publication.sax_handler.name` = "msg" [static]

Definition at line 349 of file `publication.py`.

10.126.2.2 `rpki.publication.sax_handler.pdu` = `msg` [static]

Reimplemented in [irbe_cli.publication_sax_handler](#).

Definition at line 348 of file `publication.py`.

10.126.2.3 string `rpki.publication.sax_handler.version` = "1" [static]

Definition at line 350 of file `publication.py`.

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

- [publication.py \(2493\)](#)

10.127 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.

10.127.1 Detailed Description

Container to simplify passing around the usual triple of ASN, IPv4, and IPv6 resource sets.

Definition at line 532 of file resource_set.py.

10.127.2 Member Function Documentation

10.127.2.1 `def rpki.resource_set.resource_bag.__eq__ (self, other)`

Definition at line 600 of file resource_set.py.

10.127.2.2 `def rpki.resource_set.resource_bag.__init__ (self, asn = None, v4 = None, v6 = None, valid_until = None)`

Definition at line 550 of file resource_set.py.

10.127.2.3 `def rpki.resource_set.resource_bag.__ne__ (self, other)`

Definition at line 606 of file resource_set.py.

10.127.2.4 `def rpki.resource_set.resource_bag.__str__ (self)`

Definition at line 629 of file resource_set.py.

10.127.2.5 `def rpki.resource_set.resource_bag.empty (self)`

True iff all resource sets in this bag are empty.

Definition at line 596 of file resource_set.py.

10.127.2.6 `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 573 of file resource_set.py.

10.127.2.7 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 609 of file resource_set.py.

10.127.2.8 def rpki.resource_set.resource_bag.oversized (*self*, *other*)

True iff self is oversized with respect to other.

Definition at line 556 of file resource_set.py.

10.127.2.9 def rpki.resource_set.resource_bag.undersized (*self*, *other*)

True iff self is undersized with respect to other.

Definition at line 564 of file resource_set.py.

10.127.2.10 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 619 of file resource_set.py.

10.127.3 Member Data Documentation**10.127.3.1 rpki::resource_set.resource_bag::asn**

Set of Autonomous System Number resources.

Definition at line 551 of file resource_set.py.

10.127.3.2 rpki::resource_set.resource_bag::v4

Set of IPv4 resources.

Definition at line 552 of file resource_set.py.

10.127.3.3 rpki::resource_set.resource_bag::v6

Set of IPv6 resources.

Definition at line 553 of file resource_set.py.

10.127.3.4 rpki::resource_set.resource_bag::valid_until

Expiration date of resources, for setting certificate notAfter field.

Definition at line 554 of file resource_set.py.

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

- [resource_set.py \(2457\)](#)

10.128 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](#)

10.128.1 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.

10.128.2 Member Function Documentation

10.128.2.1 def rpki.resource_set.resource_range.__cmp__ (*self*, *other*)

Compare two resource_range objects.

Definition at line 67 of file resource_set.py.

10.128.2.2 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.

10.128.3 Member Data Documentation

10.128.3.1 rpki.resource_set.resource_range.max

Definition at line 65 of file resource_set.py.

10.128.3.2 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 \(2457\)](#)

10.129 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).

10.129.1 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.

10.129.2 Member Function Documentation

10.129.2.1 `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.

10.129.2.2 `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`.

10.129.3 Member Data Documentation

10.129.3.1 `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`.

10.129.3.2 `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 \(2457\)](#)

10.130 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](#)

10.130.1 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.

10.130.2 Member Function Documentation

10.130.2.1 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.

10.130.2.2 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.

10.130.2.3 def rpki.resource_set.resource_range_ip.make_prefix (cls, address, prefixlen)

Construct a resource range corresponding to a prefix.

Definition at line 160 of file resource_set.py.

10.130.2.4 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 \(2457\)](#)

10.131 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).

10.131.1 Detailed Description

Range of IPv4 addresses.

Definition at line 170 of file resource_set.py.

10.131.2 Member Data Documentation

10.131.2.1 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 \(2457\)](#)

10.132 `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).

10.132.1 Detailed Description

Range of IPv6 addresses.

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

10.132.2 Member Data Documentation

10.132.2.1 `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 \(2457\)](#)

10.133 `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](#)

10.133.1 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.

10.133.2 Member Function Documentation

10.133.2.1 def rpki.resource_set.resource_set.__init__ (self, ini = None)

Initialize a resource_set.

Definition at line 219 of file resource_set.py.

10.133.2.2 def rpki.resource_set.resource_set.__str__ (self)

Convert a resource_set to string format.

Definition at line 246 of file resource_set.py.

10.133.2.3 `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`.

10.133.2.4 `def rpki.resource_set.resource_set.contains (self, item)`

Set membership test for resource sets.

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

10.133.2.5 `def rpki.resource_set.resource_set.difference (self, other)`

Set difference for resource sets.

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

10.133.2.6 `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 354 of file `resource_set.py`.

10.133.2.7 def rpki.resource_set.resource_set.intersection (*self*, *other*)

Set intersection for resource sets.

Definition at line 313 of file resource_set.py.

10.133.2.8 def rpki.resource_set.resource_set.issubset (*self*, *other*)

Test whether self is a subset (possibly improper) of other.

Definition at line 340 of file resource_set.py.

10.133.2.9 def rpki.resource_set.resource_set.issuperset (*self*, *other*)

Test whether self is a superset (possibly improper) of other.

Definition at line 349 of file resource_set.py.

**10.133.2.10 def rpki.resource_set.resource_set.symmetric_difference (*self*,
other)**

Set symmetric difference (XOR) for resource sets.

Definition at line 321 of file resource_set.py.

10.133.2.11 def rpki.resource_set.resource_set.union (*self*, *other*)

Set union for resource sets.

Definition at line 288 of file resource_set.py.

10.133.3 Member Data Documentation

10.133.3.1 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](#) (2457)

10.134 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](#).

10.134.1 Detailed Description

Autonomous System Number resource set.

Definition at line 369 of file `resource_set.py`.

10.134.2 Member Function Documentation

10.134.2.1 `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 389 of file resource_set.py.

10.134.2.2 `def rpki.resource_set.resource_set_as.parse_str (self, x)`

Parse ASN resource sets from text (eg, XML attributes).

Definition at line 379 of file resource_set.py.

10.134.2.3 `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 407 of file resource_set.py.

10.134.3 Member Data Documentation

10.134.3.1 `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 405 of file resource_set.py.

10.134.3.2 `rpki::resource_set.resource_set_as::range_type = resource_range_as [static]`

Type of range underlying this type of [resource_set](#).

Definition at line 377 of file resource_set.py.

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

- [resource_set.py](#) (2457)

10.135 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.

10.135.1 Detailed Description

(Generic) IP address resource set.

This is a virtual class. You probably don't want to use it directly.

Definition at line 419 of file resource_set.py.

10.135.2 Member Function Documentation

10.135.2.1 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 439 of file resource_set.py.

10.135.2.2 def rpki.resource_set.resource_set_ip.parse_str (self, x)

Parse IP address resource sets from text (eg, XML attributes).

Definition at line 427 of file resource_set.py.

10.135.2.3 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 457 of file resource_set.py.

10.135.3 Member Data Documentation

10.135.3.1 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 455 of file resource_set.py.

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

- [resource_set.py \(2457\)](#)

10.136 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](#).

10.136.1 Detailed Description

IPv4 address resource set.

Definition at line 469 of file resource_set.py.

10.136.2 Member Data Documentation

10.136.2.1 rpki::resource_set.resource_set_ipv4::afi = "\x00\x01" [static]

Address Family Identifier value for IPv4.

Definition at line 482 of file resource_set.py.

10.136.2.2 rpki::resource_set.resource_set_ipv4::range_type = resource_range_ipv4 [static]

Type of range underlying this type of [resource_set](#).

Definition at line 477 of file resource_set.py.

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

- [resource_set.py \(2457\)](#)

10.137 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](#).

10.137.1 Detailed Description

IPv6 address resource set.

Definition at line 484 of file resource_set.py.

10.137.2 Member Data Documentation

10.137.2.1 rpki::resource_set.resource_set_ipv6::afi = "\x00\x02" [static]

Address Family Identifier value for IPv6.

Definition at line 497 of file resource_set.py.

10.137.2.2 rpki::resource_set.resource_set_ipv6::range_type = resource_range_ipv6 [static]

Type of range underlying this type of [resource_set](#).

Definition at line 492 of file resource_set.py.

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

- [resource_set.py \(2457\)](#)

10.138 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

- [address](#)
Address portion of prefix.
- [max_prefixlen](#)
Maximum prefix length.
- [prefixlen](#)
(Minimum) prefix length.

10.138.1 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 651 of file `resource_set.py`.

10.138.2 Member Function Documentation

10.138.2.1 `def rpki.resource_set.roa_prefix.__cmp__(self, other)`

Compare two ROA prefix objects. Comparision is based on address, prefixlen, and max_prefixlen, in that order.

Definition at line 681 of file `resource_set.py`.

10.138.2.2 `def rpki.resource_set.roa_prefix.__init__(self, address, 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 669 of file `resource_set.py`.

10.138.2.3 def rpki.resource_set.roa_prefix.__str__ (self)

Convert a ROA prefix to string format.

Definition at line 694 of file resource_set.py.

10.138.2.4 def rpki.resource_set.roa_prefix.max (self)

Return highest address covered by prefix.

Definition at line 715 of file resource_set.py.

10.138.2.5 def rpki.resource_set.roa_prefix.min (self)

Return lowest address covered by prefix.

Definition at line 711 of file resource_set.py.

10.138.2.6 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 703 of file resource_set.py.

10.138.2.7 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 722 of file resource_set.py.

10.138.3 Member Data Documentation

10.138.3.1 rpki::resource_set.roa_prefix::address

Address portion of prefix.

Definition at line 677 of file resource_set.py.

10.138.3.2 rpki::resource_set.roa_prefix::max_prefixlen

Maximum prefix length.

Definition at line 679 of file resource_set.py.

10.138.3.3 rpki::resource_set.roa_prefix::prefixlen

(Minimum) prefix length.

Definition at line 678 of file resource_set.py.

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

- [resource_set.py \(2457\)](#)

10.139 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](#).

10.139.1 Detailed Description

IPv4 ROA prefix.

Definition at line 730 of file resource_set.py.

10.139.2 Member Data Documentation

10.139.2.1 `rpki::resource_set.roa_prefix_ipv4::range_type = resource_range_ipv4` `[static]`

Type of corresponding [resource_range_ip](#).

Definition at line 738 of file `resource_set.py`.

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

- [resource_set.py](#) (2457)

10.140 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](#).

10.140.1 Detailed Description

IPv6 ROA prefix.

Definition at line 740 of file `resource_set.py`.

10.140.2 Member Data Documentation

10.140.2.1 `rpki::resource_set.roa_prefix_ipv6::range_type = resource_range_ipv6` `[static]`

Type of corresponding [resource_range_ip](#).

Definition at line 748 of file `resource_set.py`.

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

- [resource_set.py](#) (2457)

10.141 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](#)

10.141.1 Detailed Description

Set of ROA prefixes, analogous to the `resource_set_ip` class.

Definition at line 750 of file `resource_set.py`.

10.141.2 Member Function Documentation

10.141.2.1 `def rpki.resource_set.roa_prefix_set.__init__ (self, ini = None)`

Initialize a ROA prefix set.

Definition at line 755 of file `resource_set.py`.

10.141.2.2 `def rpki.resource_set.roa_prefix_set.__str__ (self)`

Convert a ROA prefix set to string format.

Definition at line 775 of file `resource_set.py`.

10.141.2.3 `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 (address, prefixlen, max_prefixlen) triples.

Definition at line 809 of file `resource_set.py`.

10.141.2.4 `def rpki.resource_set.roa_prefix_set.parse_str (self, x)`

Parse ROA prefix from text (eg, an XML attribute).

Definition at line 779 of file `resource_set.py`.

10.141.2.5 `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 791 of file `resource_set.py`.

10.141.2.6 `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 824 of file `resource_set.py`.

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

- [resource_set.py \(2457\)](#)

10.142 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.

10.142.1 Detailed Description

Set of IPv4 ROA prefixes.

Definition at line 834 of file [resource_set.py](#).

10.142.2 Member Data Documentation

10.142.2.1 [rpki::resource_set.roa_prefix_set_ipv4::prefix_type](#) = [roa_prefix_ipv4](#) [static]

Type of underlying [roa_prefix](#).

Definition at line 842 of file [resource_set.py](#).

10.142.2.2 [rpki::resource_set.roa_prefix_set_ipv4::resource_set_type](#) = [resource_set_ipv4](#) [static]

Type of corresponding [resource_set_ip](#) class.

Definition at line 847 of file [resource_set.py](#).

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

- [resource_set.py](#) (2457)

10.143 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.

10.143.1 Detailed Description

Set of IPv6 ROA prefixes.

Definition at line 849 of file [resource_set.py](#).

10.143.2 Member Data Documentation

10.143.2.1 [rpki::resource_set.roa_prefix_set_ipv6::prefix_type](#) = [roa_prefix_ipv6](#) [static]

Type of underlying [roa_prefix](#).

Definition at line 857 of file [resource_set.py](#).

10.143.2.2 [rpki::resource_set.roa_prefix_set_ipv6::resource_set_type](#) = [resource_set_ipv6](#) [static]

Type of corresponding [resource_set_ip](#) class.

Definition at line 862 of file [resource_set.py](#).

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

- [resource_set.py](#) (2457)

10.144 rpki.roa.ROAIPAddress Class Reference

Inherits [Sequence](#).

Public Member Functions

- [def __init__](#)

Public Attributes

- [address](#)
- [maxLength](#)

10.144.1 Detailed Description

Definition at line 47 of file roa.py.

10.144.2 Member Function Documentation

10.144.2.1 `def rpki.roa.ROAIPAddress.__init__ (self, optional = 0, default = '')`

Definition at line 48 of file roa.py.

10.144.3 Member Data Documentation

10.144.3.1 `rpki.roa.ROAIPAddress.address`

Definition at line 49 of file roa.py.

10.144.3.2 `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 \(2424\)](#)

10.145 rpki.roa.ROAIPAddresses Class Reference

Inherits [SequenceOf](#).

Public Member Functions

- [def __init__](#)

10.145.1 Detailed Description

Definition at line 54 of file roa.py.

10.145.2 Member Function Documentation

10.145.2.1 `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 \(2424\)](#)

10.146 rpki.roa.ROAIPAddressFamilies Class Reference

Inherits [SequenceOf](#).

Public Member Functions

- [def __init__](#)

10.146.1 Detailed Description

Definition at line 65 of file roa.py.

10.146.2 Member Function Documentation

10.146.2.1 `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 \(2424\)](#)

10.147 rpki.roa.ROAIPAddressFamily Class Reference

Inherits [Sequence](#).

Public Member Functions

- `def __init__`

Public Attributes

- [addresses](#)
- [addressFamily](#)

10.147.1 Detailed Description

Definition at line 58 of file roa.py.

10.147.2 Member Function Documentation

10.147.2.1 `def rpki.roa.ROAIPAddressFamily.__init__ (self, optional = 0, default = "")`

Definition at line 59 of file roa.py.

10.147.3 Member Data Documentation

10.147.3.1 rpki.roa.ROAIPAddressFamily.addresses

Definition at line 61 of file roa.py.

10.147.3.2 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 \(2424\)](#)

10.148 rpki.roa.RouteOriginAttestation Class Reference

Inherits [Sequence](#).

Public Member Functions

- [def __init__](#)

Public Attributes

- [asID](#)
- [explicitVersion](#)
- [ipAddrBlocks](#)
- [version](#)

10.148.1 Detailed Description

Definition at line 69 of file roa.py.

10.148.2 Member Function Documentation

- 10.148.2.1** `def rpki.roa.RouteOriginAttestation.__init__ (self, optional = 0, default = '')`

Definition at line 70 of file roa.py.

10.148.3 Member Data Documentation

10.148.3.1 rpki.roa.RouteOriginAttestation.asID

Definition at line 73 of file roa.py.

10.148.3.2 rpki.roa.RouteOriginAttestation.explicitVersion

Definition at line 72 of file roa.py.

10.148.3.3 rpki.roa.RouteOriginAttestation.ipAddrBlocks

Definition at line 74 of file roa.py.

10.148.3.4 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 \(2424\)](#)

10.149 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 [route_origins](#)
- 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](#)

10.149.1 Detailed Description

Internal CA detail object.

Definition at line 471 of file rpki_engine.py.

10.149.2 Member Function Documentation

10.149.2.1 `def rpki.rpki_engine.ca_detail_obj.activate (self, ca, cert, uri, callback, errback, predecessor = None)`

Activate this `ca_detail`.

Definition at line 529 of file `rpki_engine.py`.

10.149.2.2 `def rpki.rpki_engine.ca_detail_obj.ca (self)`

Fetch CA object to which this `ca_detail` links.

Definition at line 501 of file `rpki_engine.py`.

10.149.2.3 `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 505 of file `rpki_engine.py`.

10.149.2.4 `def rpki.rpki_engine.ca_detail_obj.create (cls, ca)`

Create a new `ca_detail` object for a specified CA.

Definition at line 683 of file `rpki_engine.py`.

10.149.2.5 `def rpki.rpki_engine.ca_detail_obj.crl_uri (self, ca)`

Return publication URI for this `ca_detail`'s CRL.

Definition at line 517 of file `rpki_engine.py`.

10.149.2.6 `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 521 of file rpki_engine.py.

10.149.2.7 `def rpki.rpki_engine.ca_detail_obj.delete (self, ca, repository, cb, eb)`

Delete this ca_detail and all of the certs it issued.

Definition at line 562 of file rpki_engine.py.

10.149.2.8 `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 774 of file rpki_engine.py.

10.149.2.9 `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 808 of file rpki_engine.py.

10.149.2.10 `def rpki.rpki_engine.ca_detail_obj.generate_manifest_cert (self, ca)`

Generate a new manifest certificate for this ca_detail.

Definition at line 718 of file rpki_engine.py.

10.149.2.11 `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 730 of file rpki_engine.py.

10.149.2.12 `def rpki.rpki_engine.ca_detail_obj.issue_ee (self, ca, resources, subject_key, sia = None)`

Issue a new EE certificate.

Definition at line 701 of file rpki_engine.py.

10.149.2.13 `def rpki.rpki_engine.ca_detail_obj.manifest_uri (self, ca)`

Return publication URI for this ca_detail's manifest.

Definition at line 525 of file rpki_engine.py.

10.149.2.14 `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 590 of file rpki_engine.py.

10.149.2.15 def rpki.rpki_engine.ca_detail_obj.revoked_certs (self)

Fetch all revoked_cert objects that link to this ca_detail.

Definition at line 509 of file rpki_engine.py.

10.149.2.16 def rpki.rpki_engine.ca_detail_obj.route_origins (self)

Fetch all route_origin objects that link to this ca_detail.

Definition at line 513 of file rpki_engine.py.

10.149.2.17 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 491 of file rpki_engine.py.

10.149.2.18 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 654 of file rpki_engine.py.

10.149.3 Member Data Documentation

10.149.3.1 rpki.rpki_engine.ca_detail_obj.ca_cert_uri

Definition at line 535 of file rpki_engine.py.

10.149.3.2 rpki.rpki_engine.ca_detail_obj.ca_id

Definition at line 689 of file rpki_engine.py.

10.149.3.3 rpki.rpki_engine.ca_detail_obj.gctx

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 688 of file rpki_engine.py.

10.149.3.4 rpki.rpki_engine.ca_detail_obj.latest_ca_cert

Definition at line 534 of file rpki_engine.py.

10.149.3.5 rpki.rpki_engine.ca_detail_obj.latest_crl

Definition at line 798 of file rpki_engine.py.

10.149.3.6 rpki.rpki_engine.ca_detail_obj.latest_manifest

Definition at line 832 of file rpki_engine.py.

10.149.3.7 rpki.rpki_engine.ca_detail_obj.latest_manifest_cert

Definition at line 645 of file rpki_engine.py.

10.149.3.8 rpki.rpki_engine.ca_detail_obj.manifest_private_key_id

Definition at line 643 of file rpki_engine.py.

10.149.3.9 rpki.rpki_engine.ca_detail_obj.manifest_public_key

Definition at line 644 of file rpki_engine.py.

10.149.3.10 rpki.rpki_engine.ca_detail_obj.nextUpdate

Definition at line 622 of file rpki_engine.py.

10.149.3.11 rpki.rpki_engine.ca_detail_obj.private_key_id

Definition at line 642 of file rpki_engine.py.

10.149.3.12 rpki.rpki_engine.ca_detail_obj.public_key

Definition at line 693 of file rpki_engine.py.

10.149.3.13 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 476 of file rpki_engine.py.

10.149.3.14 rpki.rpki_engine.ca_detail_obj.state

Definition at line 542 of file rpki_engine.py.

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

- [rpki_engine.py \(2502\)](#)

10.150 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_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`

10.150.1 Detailed Description

Internal CA object.

Definition at line 245 of file `rpki_engine.py`.

10.150.2 Member Function Documentation

10.150.2.1 `def rpki.rpki_engine.ca_obj.ca_details (self)`

Fetch all `ca_detail` objects that link to this CA object.

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

10.150.2.2 `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 300 of file `rpki_engine.py`.

10.150.2.3 `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 287 of file `rpki_engine.py`.

10.150.2.4 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 358 of file rpki_engine.py.

10.150.2.5 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 382 of file rpki_engine.py.

10.150.2.6 def rpki.rpki_engine.ca_obj.fetch_active (self)

Fetch the active ca_detail for this CA, if any.

Definition at line 275 of file rpki_engine.py.

10.150.2.7 def rpki.rpki_engine.ca_obj.fetch_deprecated (self)

Fetch deprecated ca_details for this CA, if any.

Definition at line 279 of file rpki_engine.py.

10.150.2.8 def rpki.rpki_engine.ca_obj.fetch_pending (self)

Fetch the pending ca_details for this CA, if any.

Definition at line 271 of file rpki_engine.py.

10.150.2.9 def rpki.rpki_engine.ca_obj.fetch_revoked (*self*)

Fetch revoked ca_details for this CA, if any.

Definition at line 283 of file rpki_engine.py.

10.150.2.10 def rpki.rpki_engine.ca_obj.next_crl_number (*self*)

Allocate a CRL serial number.

Definition at line 426 of file rpki_engine.py.

10.150.2.11 def rpki.rpki_engine.ca_obj.next_manifest_number (*self*)

Allocate a manifest serial number.

Definition at line 418 of file rpki_engine.py.

10.150.2.12 def rpki.rpki_engine.ca_obj.next_serial_number (*self*)

Allocate a certificate serial number.

Definition at line 410 of file rpki_engine.py.

10.150.2.13 def rpki.rpki_engine.ca_obj.parent (*self*)

Fetch parent object to which this CA object links.

Definition at line 263 of file rpki_engine.py.

10.150.2.14 `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 434 of file rpki_engine.py.

10.150.2.15 `def rpki.rpki_engine.ca_obj.revoke (self, cb, eb)`

Revoke deprecated ca_detail objects associated with this ca.

Definition at line 459 of file rpki_engine.py.

10.150.3 Member Data Documentation**10.150.3.1** `rpki.rpki_engine.ca_obj.gctx`

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 365 of file rpki_engine.py.

10.150.3.2 `int rpki.rpki_engine.ca_obj.last_crl_sn = 0` `[static]`

Definition at line 259 of file rpki_engine.py.

10.150.3.3 `int rpki.rpki_engine.ca_obj.last_issued_sn = 0` `[static]`

Definition at line 260 of file rpki_engine.py.

10.150.3.4 `int rpki.rpki_engine.ca_obj.last_manifest_sn = 0` `[static]`

Definition at line 261 of file rpki_engine.py.

10.150.3.5 rpki.rpki_engine.ca_obj.parent_id

Definition at line 366 of file rpki_engine.py.

10.150.3.6 rpki.rpki_engine.ca_obj.parent_resource_class

Definition at line 367 of file rpki_engine.py.

10.150.3.7 rpki.rpki_engine.ca_obj.sia_uri

Definition at line 311 of file rpki_engine.py.

10.150.3.8 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 250 of file rpki_engine.py.

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

- [rpki_engine.py \(2502\)](#)

10.151 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](#)

10.151.1 Detailed Description

Certificate that has been issued to a child.

Definition at line 842 of file `rpki_engine.py`.

10.151.2 Member Function Documentation

10.151.2.1 `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 855 of file `rpki_engine.py`.

10.151.2.2 `def rpki.rpki_engine.child_cert_obj.ca_detail (self)`

Fetch `ca_detail` object to which this `child_cert` object links.

Definition at line 871 of file `rpki_engine.py`.

10.151.2.3 def rpki.rpki_engine.child_cert_obj.child (self)

Fetch child object to which this child_cert object links.

Definition at line 867 of file rpki_engine.py.

10.151.2.4 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 977 of file rpki_engine.py.

10.151.2.5 def rpki.rpki_engine.child_cert_obj.reissue (self, ca_detail, callback = None, errback = None, 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 904 of file rpki_engine.py.

10.151.2.6 def rpki.rpki_engine.child_cert_obj.revoke (self, callback, errback, withdraw = True)

Revoke a child cert.

Definition at line 883 of file rpki_engine.py.

10.151.2.7 `def rpki.rpki_engine.child_cert_obj.uri (self, ca)`

Return the publication URI for this `child_cert`.

Definition at line 879 of file `rpki_engine.py`.

10.151.2.8 `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 875 of file `rpki_engine.py`.

10.151.3 Member Data Documentation**10.151.3.1 `rpki.rpki_engine.child_cert_obj.ca_detail_id`**

Definition at line 862 of file `rpki_engine.py`.

10.151.3.2 `rpki.rpki_engine.child_cert_obj.cert`

Definition at line 863 of file `rpki_engine.py`.

10.151.3.3 `rpki.rpki_engine.child_cert_obj.child_id`

Definition at line 861 of file `rpki_engine.py`.

10.151.3.4 `rpki.rpki_engine.child_cert_obj.gctx`

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 860 of file `rpki_engine.py`.

10.151.3.5 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 847 of file rpki_engine.py.

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

- [rpki_engine.py \(2502\)](#)

10.152 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](#)

10.152.1 Detailed Description

Tombstone for a revoked certificate.

Definition at line 1009 of file rpki_engine.py.

10.152.2 Member Function Documentation

10.152.2.1 `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 1022 of file rpki_engine.py.

10.152.2.2 `def rpki.rpki_engine.revoked_cert_obj.ca_detail (self)`

Fetch `ca_detail` object to which this `revoked_cert_obj` links.

Definition at line 1033 of file rpki_engine.py.

10.152.2.3 `def rpki.rpki_engine.revoked_cert_obj.revoke (cls, cert, ca_detail)`

Revoke a certificate.

Definition at line 1038 of file rpki_engine.py.

10.152.3 Member Data Documentation

10.152.3.1 `rpki.rpki_engine.revoked_cert_obj.ca_detail_id`

Definition at line 1029 of file rpki_engine.py.

10.152.3.2 rpki.rpki_engine.revoked_cert_obj.expires

Definition at line 1028 of file rpki_engine.py.

10.152.3.3 rpki.rpki_engine.revoked_cert_obj.gctx

Reimplemented from [rpki.sql.sql_persistent](#).

Definition at line 1025 of file rpki_engine.py.

10.152.3.4 rpki.rpki_engine.revoked_cert_obj.revoked

Definition at line 1027 of file rpki_engine.py.

10.152.3.5 rpki.rpki_engine.revoked_cert_obj.serial

Definition at line 1026 of file rpki_engine.py.

10.152.3.6 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 1014 of file rpki_engine.py.

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

- [rpki_engine.py \(2502\)](#)

10.153 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 [cronjob_handler](#)
- def [irdb_query](#)
- def [irdb_query_child_resources](#)
- def [irdb_query_roa_requests](#)
- def [left_right_handler](#)
- def [up_down_handler](#)

Public Attributes

- [bpki_ta](#)
- [https_server_host](#)
- [https_server_port](#)
- [irbe_cert](#)
- [irdb_cert](#)
- [irdb_url](#)
- [publication_kludge_base](#)
- [rpkid_cert](#)
- [rpkid_key](#)
- [sql](#)

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)

10.153.1 Detailed Description

A container for various global rpkid parameters.

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

10.153.2 Member Function Documentation

10.153.2.1 `def rpki.rpki_engine.rpkid_context.__init__ (self, cfg)`

Definition at line 44 of file `rpki_engine.py`.

10.153.2.2 `def rpki.rpki_engine.rpkid_context.build_https_ta_cache (self)`

Build dynamic TLS trust anchors.

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

10.153.2.3 `def rpki.rpki_engine.rpkid_context.clear_https_ta_cache (self)`

Clear dynamic TLS trust anchors.

Definition at line 216 of file `rpki_engine.py`.

10.153.2.4 `def rpki.rpki_engine.rpkid_context.cronjob_handler (self, query, path, cb)`

Periodic tasks. This is somewhat obsolete now that we have internal timers, but the test framework still uses this, and I haven't yet refactored this code to use the new timers.

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

10.153.2.5 `def rpki.rpki_engine.rpkid_context.irdb_query (self, q_pdu, callback, errback)`

Perform an IRDB callback query.

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

10.153.2.6 `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 90 of file rpki_engine.py.

10.153.2.7 `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 110 of file rpki_engine.py.

10.153.2.8 `def rpki.rpki_engine.rpkid_context.left_right_handler (self, query, path, cb)`

Process one left-right PDU.

Definition at line 122 of file rpki_engine.py.

10.153.2.9 `def rpki.rpki_engine.rpkid_context.up_down_handler (self, query, path, cb)`

Process one up-down PDU.

Definition at line 148 of file rpki_engine.py.

10.153.3 Member Data Documentation**10.153.3.1** `rpki.rpki_engine.rpkid_context.bpki_ta`

Definition at line 48 of file rpki_engine.py.

10.153.3.2 rpki.rpki_engine.rpkid_context.https_server_host

Definition at line 56 of file rpki_engine.py.

10.153.3.3 rpki.rpki_engine.rpkid_context.https_server_port

Definition at line 57 of file rpki_engine.py.

10.153.3.4 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 214 of file rpki_engine.py.

10.153.3.5 rpki.rpki_engine.rpkid_context.irbe_cert

Definition at line 50 of file rpki_engine.py.

10.153.3.6 rpki.rpki_engine.rpkid_context.irdb_cert

Definition at line 49 of file rpki_engine.py.

10.153.3.7 rpki.rpki_engine.rpkid_context.irdb_url

Definition at line 54 of file rpki_engine.py.

10.153.3.8 rpki.rpki_engine.rpkid_context.publication_kludge_base

Definition at line 59 of file rpki_engine.py.

10.153.3.9 rpki.rpki_engine.rpkid_context.rpkid_cert

Definition at line 51 of file rpki_engine.py.

10.153.3.10 rpki.rpki_engine.rpkid_context.rpkid_key

Definition at line 52 of file rpki_engine.py.

10.153.3.11 rpki.rpki_engine.rpkid_context.sql

Definition at line 46 of file rpki_engine.py.

10.153.3.12 `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 146 of file rpki_engine.py.

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

- [rpki_engine.py \(2502\)](#)

10.154 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

10.154.1 Detailed Description

SQL session layer.

Definition at line 38 of file sql.py.

10.154.2 Member Function Documentation

10.154.2.1 def rpki.sql.session.__init__ (*self*, *cfg*)

Definition at line 45 of file sql.py.

10.154.2.2 def rpki.sql.session._wrap_execute (*self*, *func*, *query*, *args*) [private]

Definition at line 76 of file sql.py.

10.154.2.3 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.

10.154.2.4 def rpki.sql.session.cache_clear (self)

Clear the object cache.

Definition at line 96 of file sql.py.

10.154.2.5 def rpki.sql.session.close (self)

Definition at line 65 of file sql.py.

10.154.2.6 def rpki.sql.session.connect (self)

Definition at line 60 of file sql.py.

10.154.2.7 def rpki.sql.session.execute (self, query, args = None)

Definition at line 84 of file sql.py.

10.154.2.8 def rpki.sql.session.executemany (self, query, args)

Definition at line 87 of file sql.py.

10.154.2.9 def rpki.sql.session.fetchall (self)

Definition at line 90 of file sql.py.

10.154.2.10 def rpki.sql.session.lastrowid (*self*)

Definition at line 93 of file sql.py.

10.154.2.11 def rpki.sql.session.ping (*self*)

Definition at line 73 of file sql.py.

10.154.2.12 def rpki.sql.session.sweep (*self*)

Write any dirty objects out to SQL.

Definition at line 104 of file sql.py.

10.154.3 Member Data Documentation**10.154.3.1 rpki.sql.session._exceptions_enabled = False** [static, private]

Definition at line 43 of file sql.py.

10.154.3.2 rpki.sql.session.cache

Definition at line 55 of file sql.py.

10.154.3.3 rpki.sql.session.cur

Definition at line 62 of file sql.py.

10.154.3.4 rpki.sql.session.database

Definition at line 52 of file sql.py.

10.154.3.5 rpki.sql.session.db

Definition at line 61 of file sql.py.

10.154.3.6 rpki.sql.session.dirty

Definition at line 56 of file sql.py.

10.154.3.7 rpki.sql.session.password

Definition at line 53 of file sql.py.

10.154.3.8 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 \(2502\)](#)

10.155 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](#), and [rpki.rpki_engine.revoked_cert_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.

10.155.1 Detailed Description

Mixin for persistent class that needs to be stored in SQL.

Definition at line 140 of file sql.py.

10.155.2 Member Function Documentation

10.155.2.1 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 308 of file `sql.py`.

10.155.2.2 `def rpki.sql.sql_persistent.sql_delete (self)`

Delete this object from SQL.

Definition at line 281 of file `sql.py`.

10.155.2.3 `def rpki.sql.sql_persistent.sql_delete_hook (self)`

Customization hook.

Reimplemented in [rpki.left_right.route_origin_elt](#).

Definition at line 334 of file `sql.py`.

10.155.2.4 `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 295 of file `sql.py`.

10.155.2.5 `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.

10.155.2.6 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.

10.155.2.7 def rpki.sql.sql_persistent.sql_fetch_hook (self)

Customization hook.

Reimplemented in [rpki.left_right.route_origin_elt](#).

Definition at line 321 of file sql.py.

10.155.2.8 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.

10.155.2.9 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.

10.155.2.10 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.

10.155.2.11 def rpki.sql.sql_persistent.sql_insert_hook (*self*)

Customization hook.

Reimplemented in [rpki.left_right.route_origin_elt](#).

Definition at line 325 of file sql.py.

10.155.2.12 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.

10.155.2.13 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.

10.155.2.14 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.

10.155.2.15 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.

10.155.2.16 def rpki.sql.sql_persistent.sql_store (*self*)

Store this object to SQL.

Definition at line 259 of file sql.py.

10.155.2.17 def rpki.sql.sql_persistent.sql_update_hook (*self*)

Customization hook.

Definition at line 329 of file sql.py.

10.155.3 Member Data Documentation**10.155.3.1 rpki.sql.sql_persistent.gctx**

Reimplemented in [rpki.rpki_engine.ca_obj](#), [rpki.rpki_engine.ca_detail_obj](#), [rpki.rpki_engine.child_cert_obj](#), and [rpki.rpki_engine.revoked_cert_obj](#).

Definition at line 236 of file sql.py.

10.155.3.2 rpki::sql.sql_persistent::sql_debug = False [static]

Enable logging of SQL actions.

Definition at line 158 of file sql.py.

10.155.3.3 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.

10.155.3.4 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 \(2502\)](#)

10.156 rpki.sql.template Class Reference

Inherits [object](#).

Public Member Functions

- [def __init__](#)

Public Attributes

- [columns](#)
- [delete](#)
- [index](#)
- [insert](#)
- [map](#)
- [select](#)
- [table](#)
- [update](#)

10.156.1 Detailed Description

SQL template generator.

Definition at line 116 of file sql.py.

10.156.2 Member Function Documentation

10.156.2.1 `def rpki.sql.template.__init__ (self, table_name, index_column, data_columns)`

Build a SQL template.

Definition at line 121 of file sql.py.

10.156.3 Member Data Documentation

10.156.3.1 `rpki.sql.template.columns`

Definition at line 128 of file sql.py.

10.156.3.2 `rpki.sql.template.delete`

Definition at line 138 of file sql.py.

10.156.3.3 `rpki.sql.template.index`

Definition at line 127 of file sql.py.

10.156.3.4 `rpki.sql.template.insert`

Definition at line 131 of file sql.py.

10.156.3.5 `rpki.sql.template.map`

Definition at line 129 of file sql.py.

10.156.3.6 rpki.sql.template.select

Definition at line 130 of file sql.py.

10.156.3.7 rpki.sql.template.table

Definition at line 126 of file sql.py.

10.156.3.8 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 \(2502\)](#)

10.157 rpki.sundial.datetime Class Reference

Inherits [pydatetime::datetime](#).

Public Member Functions

- def [__add__](#)
- def [__str__](#)
- def [__sub__](#)
- def [earlier](#)
- def [from_sql](#)
- def [fromASN1tuple](#)
- def [fromdatetime](#)
- def [fromGeneralizedTime](#)
- def [fromUTCTime](#)
- def [fromXMLtime](#)
- def [later](#)
- def [to_sql](#)
- def [toASN1tuple](#)
- def [toGeneralizedTime](#)
- def [totimestamp](#)
- def [toUTCTime](#)
- def [toXMLtime](#)

Static Public Attributes

- tuple `PKIX_threshold` = `pydatetime.datetime(2050, 1, 1)`
Threshold specified in RFC 3280 for switchover from UTCTime to GeneralizedTime.

10.157.1 Detailed Description

RPKI extensions to standard `datetime.datetime` class. All work here is in UTC, so we use naive datetime objects.

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

10.157.2 Member Function Documentation

10.157.2.1 `def rpki.sundial.datetime.__add__ (self, other)`

Force correct class for timedelta results.

Definition at line 126 of file `sundial.py`.

10.157.2.2 `def rpki.sundial.datetime.__str__ (self)`

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

10.157.2.3 `def rpki.sundial.datetime.__sub__ (self, other)`

Force correct class for timedelta results.

Definition at line 136 of file `sundial.py`.

10.157.2.4 `def rpki.sundial.datetime.earlier (self, other)`

Return the earlier of two timestamps.

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

10.157.2.5 def rpki.sundial.datetime.from_sql (cls, x)

Convert from SQL storage format.

Definition at line 147 of file sundial.py.

10.157.2.6 def rpki.sundial.datetime.fromASN1tuple (cls, x)

Convert from ASN.1 tuple representation.

Definition at line 77 of file sundial.py.

10.157.2.7 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 119 of file sundial.py.

10.157.2.8 def rpki.sundial.datetime.fromGeneralizedTime (cls, x)

Convert from ASN.1 GeneralizedTime.

Definition at line 68 of file sundial.py.

10.157.2.9 def rpki.sundial.datetime.fromUTCTime (cls, x)

Convert from ASN.1 UTCTime.

Definition at line 59 of file sundial.py.

10.157.2.10 def rpki.sundial.datetime.fromXMLtime (cls, x)

Convert from XML time representation.

Definition at line 102 of file sundial.py.

10.157.2.11 def rpki.sundial.datetime.later (self, other)

Return the later of two timestamps.

Definition at line 166 of file sundial.py.

10.157.2.12 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 151 of file sundial.py.

10.157.2.13 def rpki.sundial.datetime.toASN1tuple (self)

Convert to ASN.1 tuple representation.

Definition at line 92 of file sundial.py.

10.157.2.14 def rpki.sundial.datetime.toGeneralizedTime (self)

Convert to ASN.1 GeneralizedTime.

Definition at line 72 of file sundial.py.

10.157.2.15 def rpki.sundial.datetime.timestamp (self)

Convert to seconds from epoch (like `time.time()`). Conversion method is a bit silly, but avoids time module timezone whackiness.

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

10.157.2.16 def rpki.sundial.datetime.toUTCTime (self)

Convert to ASN.1 UTCTime.

Definition at line 63 of file `sundial.py`.

10.157.2.17 def rpki.sundial.datetime.toXMLtime (self)

Convert to XML time representation.

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

10.157.3 Member Data Documentation**10.157.3.1 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 90 of file `sundial.py`.

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

- [sundial.py \(2452\)](#)

10.158 rpki.sundial.timedelta Class Reference

Inherits [pydatetime::timedelta](#).

Public Member Functions

- def [convert_to_seconds](#)
- def [fromtimedelta](#)
- def [parse](#)

Static Public Attributes

- tuple [regex](#)

Hideously ugly regular expression to parse the complex text form.

10.158.1 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 174 of file sundial.py.

10.158.2 Member Function Documentation

10.158.2.1 def rpki.sundial.timedelta.convert_to_seconds (self)

Convert a timedelta interval to seconds.

Definition at line 216 of file sundial.py.

10.158.2.2 def rpki.sundial.timedelta.fromtimedelta (cls, x)

Convert a datetime.timedelta object into this subclass.

Definition at line 221 of file sundial.py.

10.158.2.3 def rpki.sundial.timedelta.parse (cls, arg)

Parse text into a timedelta object.

Definition at line 200 of file sundial.py.

10.158.3 Member Data Documentation**10.158.3.1 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 191 of file sundial.py.

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

- [sundial.py \(2452\)](#)

10.159 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](#)

10.159.1 Detailed Description

Generic PDU object.

Virtual class, just provides some default methods.

Definition at line 43 of file up_down.py.

10.159.2 Member Function Documentation

10.159.2.1 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.

10.159.2.2 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.

10.159.2.3 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.

10.159.2.4 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.

10.159.2.5 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.

10.159.2.6 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 \(2499\)](#)

10.160 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](#)

10.160.1 Detailed Description

Up-Down protocol representation of an issued certificate.

Definition at line 128 of file up_down.py.

10.160.2 Member Function Documentation

10.160.2.1 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.

10.160.2.2 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.

10.160.2.3 **def rpki.up_down.certificate_elt.toXML (*self*)**

Generate a <certificate/> element.

Definition at line 151 of file up_down.py.

10.160.3 Member Data Documentation

10.160.3.1 **rpki.up_down.certificate_elt.cert**

Definition at line 148 of file up_down.py.

10.160.3.2 **rpki.up_down.certificate_elt.cert_url**

Definition at line 138 of file up_down.py.

10.160.3.3 **rpki.up_down.certificate_elt.req_resource_set_as**

Definition at line 139 of file up_down.py.

10.160.3.4 **rpki.up_down.certificate_elt.req_resource_set_ipv4**

Definition at line 140 of file up_down.py.

10.160.3.5 **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 \(2499\)](#)

10.161 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

10.161.1 Detailed Description

Up-Down protocol representation of a resource class.

Definition at line 160 of file up_down.py.

10.161.2 Member Function Documentation

10.161.2.1 `def rpki.up_down.class_elt.__init__ (self)`

Initialize `class_elt`.

Definition at line 167 of file `up_down.py`.

10.161.2.2 `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`.

10.161.2.3 `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`.

10.161.2.4 `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`.

10.161.2.5 `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`.

10.161.2.6 def rpki.up_down.class_elt.toXML (*self*)

Generate a <class/> element.

Definition at line 201 of file up_down.py.

10.161.3 Member Data Documentation

10.161.3.1 rpki.up_down.class_elt.cert_url

Definition at line 184 of file up_down.py.

10.161.3.2 rpki.up_down.class_elt.certs

Definition at line 170 of file up_down.py.

10.161.3.3 rpki.up_down.class_elt.class_name

Definition at line 183 of file up_down.py.

10.161.3.4 rpki.up_down.class_elt.issuer = None [static]

Definition at line 165 of file up_down.py.

10.161.3.5 rpki.up_down.class_elt.resource_set_as

Definition at line 186 of file up_down.py.

10.161.3.6 rpki.up_down.class_elt.resource_set_ipv4

Definition at line 187 of file up_down.py.

10.161.3.7 rpki.up_down.class_elt.resource_set_ipv6

Definition at line 188 of file up_down.py.

10.161.3.8 rpki.up_down.class_elt.resource_set_notafter

Definition at line 189 of file up_down.py.

10.161.3.9 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 \(2499\)](#)

10.162 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](#)

10.162.1 Detailed Description

Syntax for Up-Down protocol "list_response" and "issue_response" PDUs.

Definition at line 279 of file up_down.py.

10.162.2 Member Function Documentation

10.162.2.1 def rpki.up_down.class_response_syntax.__init__ (self)

Initialize class_response_syntax.

Definition at line 284 of file up_down.py.

10.162.2.2 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 289 of file up_down.py.

10.162.2.3 def rpki.up_down.class_response_syntax.toXML (self)

Generate payload of "list_response" and "issue_response" PDUs.

Definition at line 299 of file up_down.py.

10.162.3 Member Data Documentation

10.162.3.1 rpki.up_down.class_response_syntax.classes

Definition at line 287 of file up_down.py.

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

- [up_down.py \(2499\)](#)

10.163 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

10.163.1 Detailed Description

Class to hold a CMS-signed up-down PDU.

Definition at line 670 of file up_down.py.

10.163.2 Member Data Documentation

10.163.2.1 string rpki.up_down.cms_msg.encoding = "UTF-8" [static]

Definition at line 675 of file up_down.py.

10.163.2.2 rpki.up_down.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented in [rootd.cms_msg](#).

Definition at line 677 of file up_down.py.

10.163.2.3 rpki.up_down.cms_msg.schema = rpki.relaxng.up_down [static]

Definition at line 676 of file up_down.py.

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

- [up_down.py](#) (2499)

10.164 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](#)

10.164.1 Detailed Description

Up-Down protocol "error_response" PDU.

Definition at line 497 of file up_down.py.

10.164.2 Member Function Documentation

10.164.2.1 def rpki.up_down.error_response_pdu.__init__ (self, exception = None)

Initialize an error_response PDU from an exception object.

Definition at line 516 of file up_down.py.

10.164.2.2 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 556 of file up_down.py.

10.164.2.3 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 525 of file up_down.py.

10.164.2.4 def rpki.up_down.error_response_pdu.toXML (*self*)

Generate payload of "error_response" PDU.

Definition at line 541 of file up_down.py.

10.164.3 Member Data Documentation

10.164.3.1 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 502 of file up_down.py.

10.164.3.2 rpki.up_down.error_response_pdu.description

Definition at line 523 of file up_down.py.

10.164.3.3 dictionary `rpki.up_down.error_response_pdu.exceptions` [static]

Initial value:

```
{  
    rpki.exceptions.NoActiveCA : 1202 }
```

Definition at line 513 of file `up_down.py`.

10.164.3.4 `rpki.up_down.error_response_pdu.status`

Definition at line 522 of file `up_down.py`.

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

- [up_down.py \(2499\)](#)

10.165 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](#)

10.165.1 Detailed Description

Up-Down protocol "issue" PDU.

Definition at line 309 of file up_down.py.

10.165.2 Member Function Documentation

10.165.2.1 `def rpki.up_down.issue_pdu.endElement (self, stack, name, text)`

Handle "issue" PDU.

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

Definition at line 324 of file up_down.py.

10.165.2.2 `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 409 of file up_down.py.

10.165.2.3 `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 341 of file up_down.py.

10.165.2.4 `def rpki.up_down.issue_pdu.startElement (self, stack, name, attrs)`

Handle "issue" PDU.

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

Definition at line 314 of file up_down.py.

10.165.2.5 def rpki.up_down.issue_pdu.toXML (*self*)

Generate payload of "issue" PDU.

Definition at line 332 of file up_down.py.

10.165.3 Member Data Documentation

10.165.3.1 rpki.up_down.issue_pdu.class_name

Definition at line 319 of file up_down.py.

10.165.3.2 rpki.up_down.issue_pdu.pkcs10

Definition at line 329 of file up_down.py.

10.165.3.3 rpki.up_down.issue_pdu.req_resource_set_as

Definition at line 320 of file up_down.py.

10.165.3.4 rpki.up_down.issue_pdu.req_resource_set_ipv4

Definition at line 321 of file up_down.py.

10.165.3.5 rpki.up_down.issue_pdu.req_resource_set_ipv6

Definition at line 322 of file up_down.py.

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

- [up_down.py \(2499\)](#)

10.166 rpki.up_down.issue_response_pdu Class Reference

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

Public Member Functions

- def [check_response](#)

10.166.1 Detailed Description

Up-Down protocol "issue_response" PDU.

Definition at line 421 of file up_down.py.

10.166.2 Member Function Documentation

10.166.2.1 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 426 of file up_down.py.

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

- [up_down.py \(2499\)](#)

10.167 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](#)

10.167.1 Detailed Description

Up-Down protocol "list" PDU.

Definition at line 231 of file up_down.py.

10.167.2 Member Function Documentation

10.167.2.1 def rpki.up_down.list_pdu.query (*cls*, *parent*, *cb*, *eb*)

Send a "list" query to parent.

Definition at line 275 of file up_down.py.

10.167.2.2 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.

10.167.2.3 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 \(2499\)](#)

10.168 rpki.up_down.list_response_pdu Class Reference

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

10.168.1 Detailed Description

Up-Down protocol "list_response" PDU.

Definition at line 303 of file up_down.py.

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

- [up_down.py \(2499\)](#)

10.169 rpki.up_down.message_pdu Class Reference

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

Inherited by [rootd.message_pdu](#).

Public Member Functions

- def [__str__](#)
- 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

10.169.1 Detailed Description

Up-Down protocol message wrapper PDU.

Definition at line 563 of file up_down.py.

10.169.2 Member Function Documentation

10.169.2.1 `def rpki.up_down.message_pdu.__str__ (self)`

Convert a message PDU to a string.

Definition at line 605 of file up_down.py.

10.169.2.2 `def rpki.up_down.message_pdu.make_query (cls, payload, sender, recipient)`

Construct one message PDU.

Definition at line 645 of file up_down.py.

10.169.2.3 `def rpki.up_down.message_pdu.serve_error (self, exception)`

Generate an error_response message PDU.

Definition at line 633 of file up_down.py.

10.169.2.4 `def rpki.up_down.message_pdu.serve_top_level (self, child, callback)`

Serve one message request PDU.

Definition at line 609 of file up_down.py.

10.169.2.5 `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 589 of file up_down.py.

10.169.2.6 `def rpki.up_down.message_pdu.toXML (self)`

Generate payload of message PDU.

Definition at line 581 of file up_down.py.

10.169.3 Member Data Documentation

10.169.3.1 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 570 of file up_down.py.

10.169.3.2 `rpki.up_down.message_pdu.payload`

Definition at line 602 of file up_down.py.

10.169.3.3 rpki.up_down.message_pdu.recipient

Definition at line 600 of file up_down.py.

10.169.3.4 rpki.up_down.message_pdu.sender

Definition at line 599 of file up_down.py.

10.169.3.5 rpki.up_down.message_pdu.type

Definition at line 601 of file up_down.py.

10.169.3.6 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 579 of file up_down.py.

10.169.3.7 rpki.up_down.message_pdu.version

Definition at line 598 of file up_down.py.

10.169.3.8 int rpki.up_down.message_pdu.version = 1 [static]

Definition at line 568 of file up_down.py.

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

- [up_down.py \(2499\)](#)

10.170 rpki.up_down.multi_uri Class Reference

Inherits list.

Public Member Functions

- [def __init__](#)
- [def __str__](#)
- [def rsync](#)

10.170.1 Detailed Description

Container for a set of URIs.

Definition at line 95 of file up_down.py.

10.170.2 Member Function Documentation

10.170.2.1 `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.

10.170.2.2 `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.

10.170.2.3 `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 \(2499\)](#)

10.171 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](#)

10.171.1 Detailed Description

Up-Down protocol "revoke" PDU.

Definition at line 448 of file up_down.py.

10.171.2 Member Function Documentation

10.171.2.1 def rpki.up_down.revoke_pdu.get_SKI (*self*)

Convert g(SKI) encoding from PDU back to raw SKI.

Definition at line 453 of file up_down.py.

10.171.2.2 def rpki.up_down.revoke_pdu.query (*cls*, *ca_detail*, *cb*, *eb*)

Send a "revoke" request to parent associated with ca_detail.

Definition at line 479 of file up_down.py.

10.171.2.3 `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 457 of file `up_down.py`.

10.171.3 Member Data Documentation

10.171.3.1 `rpki.up_down.revoke_pdu.class_name`

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

Definition at line 486 of file `up_down.py`.

10.171.3.2 `rpki.up_down.revoke_pdu.ski`

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

Definition at line 487 of file `up_down.py`.

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

- [up_down.py \(2499\)](#)

10.172 rpki.up_down.revoke_response_pdu Class Reference

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

10.172.1 Detailed Description

Up-Down protocol "revoke_response" PDU.

Definition at line 490 of file `up_down.py`.

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

- [up_down.py \(2499\)](#)

10.173 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](#)

10.173.1 Detailed Description

Syntax for Up-Down protocol "revoke" and "revoke_response" PDUs.

Definition at line 434 of file up_down.py.

10.173.2 Member Function Documentation

10.173.2.1 def rpki.up_down.revoke_syntax.startElement (*self*, *stack*, *name*, *attrs*)

Handle "revoke" PDU.

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

Definition at line 439 of file up_down.py.

10.173.2.2 def rpki.up_down.revoke_syntax.toXML (*self*)

Generate payload of "revoke" PDU.

Definition at line 444 of file up_down.py.

10.173.3 Member Data Documentation

10.173.3.1 `rpki.up_down.revoke_syntax.class_name`

Reimplemented in [rpki.up_down.revoke_pdu](#).

Definition at line 441 of file `up_down.py`.

10.173.3.2 `rpki.up_down.revoke_syntax.ski`

Reimplemented in [rpki.up_down.revoke_pdu](#).

Definition at line 442 of file `up_down.py`.

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

- [up_down.py](#) (2499)

10.174 `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"

10.174.1 Detailed Description

SAX handler for Up-Down protocol.

Definition at line 661 of file `up_down.py`.

10.174.2 Member Data Documentation

10.174.2.1 string `rpki.up_down.sax_handler.name` = "message" `[static]`

Definition at line 667 of file up_down.py.

10.174.2.2 `rpki.up_down.sax_handler.pdu = message_pdu` `[static]`

Reimplemented in [rootd.sax_handler](#).

Definition at line 666 of file up_down.py.

10.174.2.3 `string rpki.up_down.sax_handler.version = "1"` `[static]`

Definition at line 668 of file up_down.py.

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

- [up_down.py](#) (2499)

10.175 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.

10.175.1 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 665 of file x509.py.

10.175.2 Member Function Documentation

10.175.2.1 `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 816 of file `x509.py`.

10.175.2.2 `def rpki.x509.CMS_object.get_content (self)`

Get the inner content of this `CMS_object`.

Definition at line 727 of file `x509.py`.

10.175.2.3 `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 706 of file `x509.py`.

10.175.2.4 `def rpki.x509.CMS_object.get_POW (self)`

Get the POW value of this `CMS_object`.

Definition at line 718 of file `x509.py`.

10.175.2.5 `def rpki.x509.CMS_object.set_content (self, content)`

Set the (inner) content of this `CMS_object`, clearing the wrapper.

Definition at line 734 of file `x509.py`.

10.175.2.6 `def rpki.x509.CMS_object.sign (self, keypair, certs, crls = None,
no_certs = False)`

Sign and wrap inner content.

Definition at line 844 of file x509.py.

10.175.2.7 `def rpki.x509.CMS_object.verify (self, ta)`

Verify CMS wrapper and store inner content.

Definition at line 741 of file x509.py.

10.175.3 Member Data Documentation

10.175.3.1 rpki.x509.CMS_object.content

Reimplemented in [rpki.x509.DER_CMS_object](#), and [rpki.x509.XML_CMS_object](#).

Definition at line 739 of file x509.py.

10.175.3.2 `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 691 of file x509.py.

10.175.3.3 rpki.x509.CMS_object.DER

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 714 of file x509.py.

10.175.3.4 `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 686 of file x509.py.

10.175.3.5 `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 680 of file x509.py.

10.175.3.6 `tuple rpki.x509.CMS_object.formats = ("DER", "POW")`
[static]

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 678 of file x509.py.

10.175.3.7 `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 679 of file x509.py.

10.175.3.8 `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 681 of file x509.py.

10.175.3.9 **rpki.x509.CMS_object.POW**

Definition at line 724 of file x509.py.

10.175.3.10 **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 704 of file x509.py.

10.175.3.11 **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 698 of file x509.py.

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

- [x509.py \(2496\)](#)

10.176 **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](#).

10.176.1 Detailed Description

Class to hold a Certificate Revocation List.

Definition at line 1044 of file x509.py.

10.176.2 Member Function Documentation

10.176.2.1 `def rpki.x509.CRL.generate (cls, keypair, issuer, serial, thisUpdate, nextUpdate, revokedCertificates, version = 1, digestType = "sha256WithRSAEncryption")`

Generate a new CRL.

Definition at line 1100 of file x509.py.

10.176.2.2 `def rpki.x509.CRL.get_DER (self)`

Get the DER value of this CRL.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 1052 of file x509.py.

10.176.2.3 def rpki.x509.CRL.get_POW (self)

Get the POW value of this CRL.

Definition at line 1067 of file x509.py.

10.176.2.4 def rpki.x509.CRL.get_POWpkix (self)

Get the POW.pkix value of this CRL.

Definition at line 1076 of file x509.py.

10.176.2.5 def rpki.x509.CRL.getIssuer (self)

Get issuer value of this CRL.

Definition at line 1095 of file x509.py.

10.176.2.6 def rpki.x509.CRL.getNextUpdate (self)

Get nextUpdate value from this CRL.

Definition at line 1091 of file x509.py.

10.176.2.7 def rpki.x509.CRL.getThisUpdate (self)

Get thisUpdate value from this CRL.

Definition at line 1087 of file x509.py.

10.176.3 Member Data Documentation

10.176.3.1 rpki.x509.CRL.DER

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 1060 of file x509.py.

10.176.3.2 `tuple rpki.x509.CRL.formats = ("DER", "POW", "POWpkix")`
`[static]`

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 1049 of file x509.py.

10.176.3.3 `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 1050 of file x509.py.

10.176.3.4 rpki.x509.CRL.POW

Definition at line 1073 of file x509.py.

10.176.3.5 rpki.x509.CRL.POWpkix

Definition at line 1084 of file x509.py.

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

- [x509.py \(2496\)](#)

10.177 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](#)

10.177.1 Detailed Description

Class to hold CMS objects with DER-based content.

Definition at line 880 of file x509.py.

10.177.2 Member Function Documentation

10.177.2.1 def rpki.x509.DER_CMS_object.decode (self, der)

Decode DER and set inner content.

Definition at line 889 of file x509.py.

10.177.2.2 def rpki.x509.DER_CMS_object.encode (self)

Encode inner content for signing.

Definition at line 885 of file x509.py.

10.177.3 Member Data Documentation

10.177.3.1 rpki.x509.DER_CMS_object.content

Reimplemented from [rpki.x509.CMS_object](#).

Definition at line 895 of file x509.py.

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

- [x509.py \(2496\)](#)

10.178 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](#).

10.178.1 Detailed Description

Virtual class to hold a generic DER object.

Definition at line 104 of file x509.py.

10.178.2 Member Function Documentation

10.178.2.1 def rpki.x509.DER_object.__cmp__(self, other)

Compare two DER-encoded objects.

Definition at line 199 of file x509.py.

10.178.2.2 def rpki.x509.DER_object.__init__(self, kw)

Initialize a DER_object.

Definition at line 137 of file x509.py.

10.178.2.3 def rpki.x509.DER_object.clear (self)

Make this object empty.

Definition at line 130 of file x509.py.

10.178.2.4 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 298 of file x509.py.

10.178.2.5 def rpki.x509.DER_object.empty (self)

Test whether this object is empty.

Definition at line 121 of file x509.py.

10.178.2.6 def rpki.x509.DER_object.from_sql (cls, x)

Convert from SQL storage format.

Definition at line 290 of file x509.py.

10.178.2.7 def rpki.x509.DER_object.gAKI (self)

Calculate g(AKI) for this object. Only work for subclasses
that implement get_AKI().

Definition at line 226 of file x509.py.

10.178.2.8 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 277 of file x509.py.

10.178.2.9 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 255 of file x509.py.

10.178.2.10 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 233 of file x509.py.

10.178.2.11 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.

10.178.2.12 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 262 of file x509.py.

10.178.2.13 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.

10.178.2.14 def rpki.x509.DER_object.get_PEM (self)

Get the PEM representation of this object.

Definition at line 195 of file x509.py.

10.178.2.15 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 248 of file x509.py.

10.178.2.16 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 241 of file x509.py.

10.178.2.17 def rpki.x509.DER_object.gSKI (self)

Calculate g(SKI) for this object. Only work for subclasses that implement get_SKI().

Definition at line 211 of file x509.py.

10.178.2.18 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 218 of file x509.py.

10.178.2.19 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 203 of file x509.py.

10.178.2.20 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 269 of file x509.py.

10.178.2.21 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.

10.178.2.22 def rpki.x509.DER_object.to_sql (self)

Convert to SQL storage format.

Definition at line 294 of file x509.py.

10.178.3 Member Data Documentation

10.178.3.1 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.

10.178.3.2 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.

10.178.3.3 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.

10.178.3.4 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 \(2496\)](#)

10.179 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](#)

10.179.1 Detailed Description

Convert between DER and PEM encodings for various kinds of ASN.1 data.

Definition at line 61 of file x509.py.

10.179.2 Member Function Documentation

10.179.2.1 `def rpki.x509.PEM_converter.__init__ (self, kind)`

Initialize PEM_converter.

Definition at line 66 of file x509.py.

10.179.2.2 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.

10.179.2.3 def rpki.x509.PEM_converter.to_DER (self, pem)

Convert from PEM to DER.

Definition at line 80 of file x509.py.

10.179.2.4 def rpki.x509.PEM_converter.to_PEM (self, der)

Convert from DER to PEM.

Definition at line 93 of file x509.py.

10.179.3 Member Data Documentation**10.179.3.1 rpki.x509.PEM_converter.b**

Definition at line 70 of file x509.py.

10.179.3.2 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 \(2496\)](#)

10.180 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](#).

10.180.1 Detailed Description

Class to hold a PKCS #10 request.

Definition at line 464 of file x509.py.

10.180.2 Member Function Documentation

10.180.2.1 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 499 of file x509.py.

10.180.2.2 def rpki.x509.PKCS10.create (cls, keypair, exts = None)

Create a new request for a given keypair, including given extensions.

Definition at line 559 of file x509.py.

10.180.2.3 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 546 of file x509.py.

10.180.2.4 def rpki.x509.PKCS10.get_DER (self)

Get the DER value of this certification request.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 472 of file x509.py.

10.180.2.5 def rpki.x509.PKCS10.get_POWpkix (self)

Get the POW.pkix value of this certification request.

Definition at line 484 of file x509.py.

10.180.2.6 def rpki.x509.PKCS10.getPublicKey (*self*)

Extract the public key from this certification request.

Definition at line 495 of file x509.py.

10.180.3 Member Data Documentation

10.180.3.1 rpki.x509.PKCS10.DER

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 480 of file x509.py.

10.180.3.2 tuple rpki.x509.PKCS10.formats = ("DER", "POWpkix") [static]

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 469 of file x509.py.

10.180.3.3 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 470 of file x509.py.

10.180.3.4 rpki.x509.PKCS10.POWpkix

Definition at line 492 of file x509.py.

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

- [x509.py \(2496\)](#)

10.181 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](#).

10.181.1 Detailed Description

Class to hold a signed ROA.

Definition at line 937 of file x509.py.

10.181.2 Member Function Documentation

10.181.2.1 def rpki.x509.ROA.build (cls, as_number, ipv4, ipv6, keypair, certs, version = 0)

Build a ROA.

Definition at line 947 of file x509.py.

10.181.3 Member Data Documentation

10.181.3.1 rpki.x509.ROA.content_class = rpki.roa.RouteOriginAttestation [static]

Definition at line 943 of file x509.py.

10.181.3.2 `tuple rpki.x509.ROA.econtent_oid = POWify_OID("id-ct-routeOriginAttestation")` `[static]`

Reimplemented from [rpki.x509.CMS_object](#).

Definition at line 944 of file x509.py.

10.181.3.3 `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 942 of file x509.py.

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

- [x509.py](#) (2496)

10.182 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](#).

10.182.1 Detailed Description

Class to hold an RSA key pair.

Definition at line 573 of file x509.py.

10.182.2 Member Function Documentation

10.182.2.1 `def rpki.x509.RSA.generate (cls, keylength = 2048)`

Generate a new keypair.

Definition at line 603 of file x509.py.

10.182.2.2 `def rpki.x509.RSA.get_DER (self)`

Get the DER value of this keypair.

Reimplemented from `rpki.x509.DER_object`.

Definition at line 581 of file x509.py.

10.182.2.3 `def rpki.x509.RSA.get_POW (self)`

Get the POW value of this keypair.

Definition at line 593 of file x509.py.

10.182.2.4 def rpki.x509.RSA.get_public_DER (self)

Get the DER encoding of the public key from this keypair.

Definition at line 610 of file x509.py.

10.182.2.5 def rpki.x509.RSA.get_RSAPublic (self)

Convert the public key of this keypair into a RSAPublic object.

Definition at line 618 of file x509.py.

10.182.2.6 def rpki.x509.RSA.get_SKI (self)

Calculate the SKI of this keypair.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 614 of file x509.py.

10.182.3 Member Data Documentation**10.182.3.1 rpki.x509.RSA.DER**

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 589 of file x509.py.

10.182.3.2 tuple rpki.x509.RSA.formats = ("DER", "POW") [static]

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 578 of file x509.py.

10.182.3.3 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 579 of file `x509.py`.

10.182.3.4 rpki.x509.RSA.POW

Definition at line 599 of file `x509.py`.

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

- [x509.py](#) (2496)

10.183 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](#).

10.183.1 Detailed Description

Class to hold an RSA public key.

Definition at line 622 of file x509.py.

10.183.2 Member Function Documentation

10.183.2.1 def rpki.x509.RSAPublic.get_DER (*self*)

Get the DER value of this public key.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 630 of file x509.py.

10.183.2.2 def rpki.x509.RSAPublic.get_POW (*self*)

Get the POW value of this public key.

Definition at line 642 of file x509.py.

10.183.2.3 def rpki.x509.RSAPublic.get_SKI (*self*)

Calculate the SKI of this public key.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 651 of file x509.py.

10.183.3 Member Data Documentation

10.183.3.1 rpki.x509.RSAPublic.DER

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 638 of file x509.py.

10.183.3.2 tuple rpki.x509.RSAPublic.formats = ("DER", "POW") [static]

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 627 of file x509.py.

10.183.3.3 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 628 of file x509.py.

10.183.3.4 rpki.x509.RSAPublic.POW

Definition at line 648 of file x509.py.

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

- [x509.py \(2496\)](#)

10.184 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](#).

10.184.1 Detailed Description

Class to hold a signed manifest.

Definition at line 897 of file x509.py.

10.184.2 Member Function Documentation

10.184.2.1 `def rpki.x509.SignedManifest.build (cls, serial, thisUpdate, nextUpdate, names_and_objs, keypair, certs, version = 0)`

Build a signed manifest.

Definition at line 915 of file x509.py.

10.184.2.2 `def rpki.x509.SignedManifest.getNextUpdate (self)`

Get nextUpdate value from this manifest.

Definition at line 910 of file x509.py.

10.184.2.3 `def rpki.x509.SignedManifest.getThisUpdate (self)`

Get thisUpdate value from this manifest.

Definition at line 906 of file x509.py.

10.184.3 Member Data Documentation**10.184.3.1** `rpki.x509.SignedManifest.content_class = rpki.manifest.Manifest
[static]`

Definition at line 903 of file x509.py.

10.184.3.2 `tuple rpki.x509.SignedManifest.econtent_oid =
POWify_OID("id-ct-rpkiManifest") [static]`

Reimplemented from [rpki.x509.CMS_object](#).

Definition at line 904 of file x509.py.

10.184.3.3 `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 902 of file x509.py.

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

- [x509.py \(2496\)](#)

10.185 rpki.x509.X509 Class Reference

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

Public Member Functions

- 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`.

10.185.1 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 318 of file `x509.py`.

10.185.2 Member Function Documentation

10.185.2.1 def rpki.x509.X509.expired (*self*)

Test whether this certificate has expired.

Definition at line 391 of file x509.py.

10.185.2.2 def rpki.x509.X509.get_DER (*self*)

Get the DER value of this certificate.

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 332 of file x509.py.

10.185.2.3 def rpki.x509.X509.get_POW (*self*)

Get the POW value of this certificate.

Definition at line 347 of file x509.py.

10.185.2.4 def rpki.x509.X509.get_POWpkix (*self*)

Get the POW.pkix value of this certificate.

Definition at line 356 of file x509.py.

10.185.2.5 def rpki.x509.X509.getIssuer (*self*)

Get the issuer of this certificate.

Definition at line 367 of file x509.py.

10.185.2.6 def rpki.x509.X509.getNotAfter (self)

Get the expiration time of this certificate.

Definition at line 379 of file x509.py.

10.185.2.7 def rpki.x509.X509.getNotBefore (self)

Get the inception time of this certificate.

Definition at line 375 of file x509.py.

10.185.2.8 def rpki.x509.X509.getPublicKey (self)

Extract the public key from this certificate.

Definition at line 387 of file x509.py.

10.185.2.9 def rpki.x509.X509.getSerial (self)

Get the serial number of this certificate.

Definition at line 383 of file x509.py.

10.185.2.10 def rpki.x509.X509.getSubject (self)

Get the subject of this certificate.

Definition at line 371 of file x509.py.

10.185.2.11 `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 395 of file x509.py.

10.185.2.12 `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 451 of file x509.py.

10.185.3 Member Data Documentation

10.185.3.1 `rpki.x509.X509.DER`

DER value of this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 340 of file x509.py.

10.185.3.2 `tuple rpki.x509.X509.formats = ("DER", "POW", "POWpkix")`
`[static]`

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 329 of file x509.py.

10.185.3.3 tuple rpki.x509.X509.pem_converter =
 PEM_converter("CERTIFICATE") [static]

PEM converter for this [object](#).

Reimplemented from [rpki.x509.DER_object](#).

Definition at line 330 of file x509.py.

10.185.3.4 rpki.x509.X509.POW

Definition at line 353 of file x509.py.

10.185.3.5 rpki.x509.X509.POWpkix

Definition at line 364 of file x509.py.

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

- [x509.py \(2496\)](#)

10.186 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")

10.186.1 Detailed Description

Class to hold CMS-wrapped XML protocol data.

Definition at line 960 of file x509.py.

10.186.2 Member Function Documentation

10.186.2.1 def rpki.x509.XML_CMS_object.decode (self, xml)

Decode XML and set inner content.

Definition at line 985 of file x509.py.

10.186.2.2 def rpki.x509.XML_CMS_object.dump_to_disk (self, prefix)

Write DER of current message to disk, for debugging.

Definition at line 1003 of file x509.py.

10.186.2.3 def rpki.x509.XML_CMS_object.encode (self)

Encode inner content for signing.

Definition at line 981 of file x509.py.

10.186.2.4 `def rpki.x509.XML_CMS_object.pretty_print_content (self)`

Pretty print XML content of this message.

Definition at line 989 of file x509.py.

10.186.2.5 `def rpki.x509.XML_CMS_object.schema_check (self)`

Handle XML RelaxNG schema check.

Definition at line 993 of file x509.py.

10.186.2.6 `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 1029 of file x509.py.

10.186.2.7 `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 1012 of file x509.py.

10.186.3 Member Data Documentation**10.186.3.1** `rpki.x509.XML_CMS_object.content`

Reimplemented from [rpki.x509.CMS_object](#).

Definition at line 987 of file x509.py.

10.186.3.2 `rpki.x509.XML_CMS_object.dump_inbound_cms = None`
[static]

Definition at line 979 of file x509.py.

10.186.3.3 `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 972 of file x509.py.

10.186.3.4 `tuple rpki.x509.XML_CMS_object.econtent_oid =`
`POWify_OID("id-ct-xml")` [static]

Reimplemented from [rpki.x509.CMS_object](#).

Definition at line 965 of file x509.py.

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

- [x509.py \(2496\)](#)

10.187 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.left_right.report_error_elt](#), [rpki.publication.publication_object_elt](#), [rpki.publication.report_error_elt](#), and [rpki.xml_utils.data_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.

10.187.1 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.

10.187.2 Member Function Documentation

10.187.2.1 def rpki.xml_utils.base_elt.__str__ (self)

Convert a base_elt object to string format.

Definition at line 201 of file xml_utils.py.

10.187.2.2 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](#), and [rpki.xml_utils.data_elt](#).

Definition at line 153 of file xml_utils.py.

10.187.2.3 `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.

10.187.2.4 `def rpki.xml_utils.base_elt.make_elt (self)`

XML element constructor.

Definition at line 178 of file xml_utils.py.

10.187.2.5 `def rpki.xml_utils.base_elt.make_pdu (cls, kargs)`

Generic PDU constructor.

Definition at line 208 of file xml_utils.py.

10.187.2.6 `def rpki.xml_utils.base_elt.read_attrs (self, attrs)`

Template-driven attribute reader.

Definition at line 166 of file xml_utils.py.

10.187.2.7 `def rpki.xml_utils.base_elt.startElement (self, stack, name, attrs)`

Default startElement() handler: just process attributes.

Reimplemented in [rpki.left_right.route_origin_elt](#), [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.

10.187.2.8 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](#), and [rpki.xml_utils.data_elt](#).

Definition at line 160 of file xml_utils.py.

10.187.3 Member Data Documentation

10.187.3.1 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.route_origin_elt](#), [rpki.left_right.list_resources_elt](#), [rpki.left_right.list_roa_requests_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.

10.187.3.2 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](#), [rpki.left_right.child_elt](#), and [rpki.left_right.route_origin_elt](#).

Definition at line 143 of file xml_utils.py.

10.187.3.3 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 \(2493\)](#)

10.188 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_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](#)

10.188.1 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 219 of file xml_utils.py.

10.188.2 Member Function Documentation

10.188.2.1 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 225 of file `xml_utils.py`.

10.188.2.2 `def rpki.xml_utils.data_elt.make_reply (self, r_pdu = None)`

Construct a reply PDU.

Definition at line 251 of file `xml_utils.py`.

10.188.2.3 `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 267 of file `xml_utils.py`.

10.188.2.4 `def rpki.xml_utils.data_elt.serve_create (self, r_msg, cb, eb)`

Handle a create action.

Definition at line 289 of file `xml_utils.py`.

10.188.2.5 `def rpki.xml_utils.data_elt.serve_destroy (self, r_msg, cb, eb)`

Handle a destroy action.

Definition at line 351 of file `xml_utils.py`.

10.188.2.6 `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 360 of file `xml_utils.py`.

10.188.2.7 `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 271 of file `xml_utils.py`.

10.188.2.8 `def rpki.xml_utils.data_elt.serve_get (self, r_msg, cb, eb)`

Handle a `get` action.

Definition at line 333 of file `xml_utils.py`.

10.188.2.9 `def rpki.xml_utils.data_elt.serve_list (self, r_msg, cb, eb)`

Handle a `list` action for non-self objects.

Definition at line 342 of file `xml_utils.py`.

10.188.2.10 `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](#), [rpki.left_right.route_origin_elt](#), and [rpki.publication.client_elt](#).

Definition at line 285 of file `xml_utils.py`.

10.188.2.11 `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 281 of file `xml_utils.py`.

10.188.2.12 `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 310 of file `xml_utils.py`.

10.188.2.13 `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 239 of file `xml_utils.py`.

10.188.2.14 `def rpki.xml_utils.data_elt.unimplemented_control (self, controls)`

Uniform handling for unimplemented control operations.

Reimplemented in [rpki.left_right.data_elt](#).

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

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

- [xml_utils.py \(2493\)](#)

10.189 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 [startElement](#)
- def [toXML](#)

Public Attributes

- [type](#)
- [version](#)

10.189.1 Detailed Description

Generic top-level PDU.

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

10.189.2 Member Function Documentation

10.189.2.1 def rpki.xml_utils.msg.__str__ (*self*)

Convert msg object to string.

Definition at line 407 of file `xml_utils.py`.

10.189.2.2 def rpki.xml_utils.msg.endElement (*self*, *stack*, *name*, *text*)

Handle top-level PDU.

Definition at line 399 of file `xml_utils.py`.

10.189.2.3 def rpki.xml_utils.msg.startElement (self, stack, name, attrs)

Handle top-level PDU.

Definition at line 386 of file xml_utils.py.

10.189.2.4 def rpki.xml_utils.msg.toXML (self)

Generate top-level PDU.

Definition at line 411 of file xml_utils.py.

10.189.3 Member Data Documentation

10.189.3.1 rpki.xml_utils.msg.type

Definition at line 392 of file xml_utils.py.

10.189.3.2 rpki.xml_utils.msg.version

Reimplemented in [rpki.left_right.msg](#), and [rpki.publication.msg](#).

Definition at line 391 of file xml_utils.py.

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

- [xml_utils.py](#) (2493)

10.190 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](#)

10.190.1 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.

10.190.2 Member Function Documentation

10.190.2.1 def rpki.xml_utils.sax_handler.__init__ (*self*)

Initialize SAX handler.

Definition at line 53 of file xml_utils.py.

10.190.2.2 `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.

10.190.2.3 `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.

10.190.2.4 `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.

10.190.2.5 `def rpki.xml_utils.sax_handler.endElementNS (self, name, qname)`

Redirect endElementNS() events to endElement().

Definition at line 65 of file xml_utils.py.

10.190.2.6 `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.

10.190.2.7 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.

10.190.2.8 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.

10.190.3 Member Data Documentation**10.190.3.1 rpki.xml_utils.sax_handler.result**

Definition at line 97 of file xml_utils.py.

10.190.3.2 rpki.xml_utils.sax_handler.stack

Definition at line 59 of file xml_utils.py.

10.190.3.3 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 \(2493\)](#)

10.191 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 \(2424\)](#)

10.192 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 \(2424\)](#)

10.193 textwrap.TextWrapper Class Reference

Inherited by [irbe_cli.UsageWrapper](#).

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

- [irbe_cli.py \(2452\)](#)

10.194 xml.sax.handler.ContentHandler Class Reference

Inherited by [rpki.xml_utils.sax_handler](#).

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

- [xml_utils.py \(2493\)](#)

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.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 `cross_certify.py` File Reference

Packages

- package `cross_certify`

Functions

- def `cross_certify.make_ext`
- def `cross_certify.usage`

Variables

- tuple `cross_certify.cert` = `rpki.x509.X509(POWpkix = x)`
- `cross_certify.child` = `None`
- `cross_certify.critical` = `False`,
- tuple `cross_certify.f` = `open(serial_file, "r")`
- `cross_certify.keypair` = `None`
- tuple `cross_certify.lifetime` = `rpki.sundial.timedelta(days = 30)`
- `cross_certify.notAfter` = `now+lifetime`
- tuple `cross_certify.now` = `rpki.sundial.now()`
- `cross_certify.output` = `None`
- `cross_certify.parent` = `None`
- tuple `cross_certify.serial` = `f.read()`
- `cross_certify.serial_file` = `None`
- tuple `cross_certify.value` = `child.get_SKI()`
- tuple `cross_certify.x` = `POW.pkix.Certificate()`

11.5 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.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.ForbiddenURI](#)
- class [rpki.exceptions.HTTPRequestFailed](#)
- class [rpki.exceptions.HTTPSClientAborted](#)
- class [rpki.exceptions.MissingCMSCRL](#)
- class [rpki.exceptions.MissingCMSEECert](#)
- class [rpki.exceptions.MultipleTLSEECert](#)
- class [rpki.exceptions.MustBePrefix](#)
- class [rpki.exceptions.NoActiveCA](#)
- 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](#)

11.6 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](#) = False
- [rpki::https.debug_tls_certs](#) = False
- tuple [rpki::https.default_http_version](#) = (1, 0)
- tuple [rpki::https.default_timeout](#) = [rpki.sundial.timedelta](#)(seconds = 90)
- string [rpki::https.rpki_content_type](#) = "application/x-rpki"
- [rpki::https.want_persistent_client](#) = True
- [rpki::https.want_persistent_server](#) = True

11.7 ipaddrs.py File Reference

Classes

- class [rpki.ipaddrs.v4addr](#)
- class [rpki.ipaddrs.v6addr](#)

Packages

- package [rpki.ipaddrs](#)

11.8 irbe_cli.py File Reference

Classes

- class [irbe_cli.bsc_elt](#)
- class [irbe_cli.certificate_elt](#)
- class [irbe_cli.child_elt](#)
- class [irbe_cli.client_elt](#)

- class [irbe_cli.cmd_elt_mixin](#)
- class [irbe_cli.cmd_msg_mixin](#)
- class [irbe_cli.config_elt](#)
- class [irbe_cli.crl_elt](#)
- class [irbe_cli.left_right_cms_msg](#)
- class [irbe_cli.left_right_msg](#)
- class [irbe_cli.left_right_sax_handler](#)
- 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.repository_elt](#)
- class [irbe_cli.roa_elt](#)
- class [irbe_cli.route_origin_elt](#)
- class [irbe_cli.self_elt](#)
- class [irbe_cli.UsageWrapper](#)

Packages

- package [irbe_cli](#)

Functions

- def [irbe_cli.call_daemon](#)
- def [irbe_cli.usage](#)

Variables

- list [irbe_cli.argv](#) = sys.argv[1:]
- tuple [irbe_cli.cfg](#) = [rpki.config.parser](#)(cfg_file, "irbe_cli")
- string [irbe_cli.cfg_file](#) = "irbe.conf"
- tuple [irbe_cli.client_cert](#) = [rpki.x509.X509](#)(Auto_file = cfg.get("rpkid-irbe-cert"))
- tuple [irbe_cli.client_key](#) = [rpki.x509.RSA](#)(Auto_file = cfg.get("rpkid-irbe-key"))
- [irbe_cli.cms_class](#) = [left_right_cms_msg](#),
- [irbe_cli.pem_out](#) = None
- [irbe_cli.q_msg](#) = [q_msg_left_right](#)
- tuple [irbe_cli.q_msg_left_right](#) = [left_right_msg](#)()
- tuple [irbe_cli.q_msg_publication](#) = [publication_msg](#)()
- list [irbe_cli.q_pdu](#) = [left_right_msg.pdus](#)[argv[0]]

- tuple [irbe_cli.server_ta](#)
- list [irbe_cli.top_opts](#) = ["config=", "help", "pem_out=", "verbose"]
- tuple [irbe_cli.url](#) = [cfg.get\("rpki-url"\)](#)
- tuple [irbe_cli.usage_fill](#) = [UsageWrapper\(subsequent_indent = " " * 4\)](#)
- [irbe_cli.verbose](#) = False

11.9 irdbd.py File Reference

Packages

- package [irdbd](#)

Functions

- 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](#), [rpki_cert](#))
- tuple [irdbd.cur](#) = [db.cursor\(\)](#)
- tuple [irdbd.db](#)
- 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.rpki_cert](#) = [rpki.x509.X509](#)(Auto_file = [cfg.get\("rpki-cert"\)](#))
- [irdbd.server_cert](#) = [irdbd_cert](#),
- tuple [irdbd.startup_msg](#) = [cfg.get\("startup-message", ""\)](#)
- tuple [irdbd.u](#) = [urlparse.urlparse](#)([cfg.get\("https-url"\)](#))

11.10 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_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.route_origin_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

11.11 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](#)

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)`

11.12 manifest.py File Reference

Classes

- class `rpki.manifest.FileAndHash`
- class `rpki.manifest.FilesAndHashes`
- class `rpki.manifest.Manifest`

Packages

- package `rpki.manifest`

11.13 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.

11.14 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

11.15 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](#)

Variables

- tuple `rpki::publication.obj2elt` = dict((e.payload_type, e) for e in (certificate_elt, crl_elt, manifest_elt, roa_elt))

Map of data types to `publication` element wrapper types.

11.16 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.

11.17 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.

11.18 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](#)

11.19 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.get_subject_cert](#)
- def [rootd.get_subject_pkcs10](#)
- def [rootd.issue_subject_cert_maybe](#)
- 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")`
- tuple `rootd.rpki_root_cert` = `rpki.x509.X509`(`Auto_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", "Subroot.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", "Subroot.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`,

11.20 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.rpkid_context`

Packages

- package `rpki.rpki_engine`

11.21 rpkid.py File Reference

Packages

- package `rpkid`

Functions

- def [rpkid.main](#)

Variables

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

11.22 sql.py File Reference**Classes**

- class [rpki.sql.session](#)
- class [rpki.sql.sql_persistent](#)
- class [rpki.sql.template](#)

Packages

- package [rpki.sql](#)

11.23 sundial.py File Reference**Classes**

- class [rpki.sundial.datetime](#)
- class [rpki.sundial.timedelta](#)

Packages

- package [rpki.sundial](#)

Functions

- def [rpki::sundial.now](#)
- def [rpki::sundial.test](#)

11.24 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/"

11.25 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](#)

11.26 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](#)

Packages

- package [rpki.xml_utils](#)

Index

- `__add__`
 - `rpki::sundial::datetime`, 307
- `__call__`
 - `irbe_cli::UsageWrapper`, 113
 - `rpki::async::iterator`, 123
 - `rpki::log::logger`, 216
- `__cmp__`
 - `rpki::async::timer`, 125
 - `rpki::resource_set::resource_range`, 243
 - `rpki::resource_set::roa_prefix`, 258
 - `rpki::x509::DER_object`, 350
- `__eq__`
 - `rpki::resource_set::resource_bag`, 240
- `__init__`
 - `pubd::pubd_context`, 115
 - `rpki::async::iterator`, 123
 - `rpki::async::timer`, 125
 - `rpki::config::parser`, 129
 - `rpki::https::http_client`, 147
 - `rpki::https::http_listener`, 151
 - `rpki::https::http_message`, 153
 - `rpki::https::http_queue`, 156
 - `rpki::https::http_request`, 158
 - `rpki::https::http_response`, 160
 - `rpki::https::http_server`, 162
 - `rpki::https::http_stream`, 165
 - `rpki::log::logger`, 216
 - `rpki::manifest::FileAndHash`, 217
 - `rpki::manifest::FilesAndHashes`, 218
 - `rpki::manifest::Manifest`, 219
 - `rpki::resource_set::resource_bag`, 240
 - `rpki::resource_set::resource_range`, 243
 - `rpki::resource_set::resource_set`, 249
 - `rpki::resource_set::roa_prefix`, 258
 - `rpki::resource_set::roa_prefix_set`, 262
 - `rpki::roa::ROAIPAddress`, 266
 - `rpki::roa::ROAIPAddresses`, 267
 - `rpki::roa::ROAIPAddressFamilies`, 268
 - `rpki::roa::ROAIPAddressFamily`, 268
 - `rpki::roa::RouteOriginAttestation`, 269
 - `rpki::rpki_engine::child_cert_obj`, 284
 - `rpki::rpki_engine::revoked_cert_obj`, 288
 - `rpki::rpki_engine::rpkid_context`, 291
 - `rpki::sql::session`, 295
 - `rpki::sql::template`, 305
 - `rpki::up_down::class_elt`, 318
 - `rpki::up_down::class_response_-syntax`, 321
 - `rpki::up_down::error_response_pdu`, 323
 - `rpki::up_down::multi_uri`, 334
 - `rpki::x509::DER_object`, 350
 - `rpki::x509::PEM_converter`, 356
 - `rpki::xml_utils::sax_handler`, 387
- `__init__.py(2496)`, 390
- `__ne__`
 - `rpki::resource_set::resource_bag`, 240
- `__new__`
 - `rpki::ipaddrs::v4addr`, 170
 - `rpki::ipaddrs::v6addr`, 172
- `__repr__`
 - `rpki::async::iterator`, 123
 - `rpki::async::timer`, 126
- `__str__`
 - `rpki::https::http_message`, 153
 - `rpki::ipaddrs::v4addr`, 170
 - `rpki::ipaddrs::v6addr`, 172
 - `rpki::resource_set::resource_bag`, 240
 - `rpki::resource_set::resource_range_-as`, 244
 - `rpki::resource_set::resource_range_-`

- ip, 246
- rpki::resource_set::resource_set, 249
- rpki::resource_set::roa_prefix, 258
- rpki::resource_set::roa_prefix_set, 262
- rpki::sundial::datetime, 307
- rpki::up_down::message_pdu, 331
- rpki::up_down::multi_uri, 334
- rpki::xml_utils::base_elt, 378
- rpki::xml_utils::msg, 385
- _sub_
 - rpki::sundial::datetime, 307
- _bs2long
 - rpki::resource_set, 85
- _comm
 - rpki::resource_set::resource_set, 249
- _exceptions_enabled
 - rpki::sql::session, 297
- _long2bs
 - rpki::resource_set, 85
- _prefixlen
 - rpki::resource_set::resource_range_ - ip, 246
- _raiseExitNow
 - rpki::async, 67
- _rsplit
 - rpki::resource_set, 86
- _wrap_execute
 - rpki::sql::session, 295
- activate
 - rpki::rpki_engine::ca_detail_obj, 272
- address
 - rpki::resource_set::roa_prefix, 260
 - rpki::roa::ROAIPAddress, 266
- addresses
 - rpki::roa::ROAIPAddressFamily, 269
- addressFamily
 - rpki::roa::ROAIPAddressFamily, 269
- afi
 - rpki::resource_set::resource_set_ - ipv4, 256
 - rpki::resource_set::resource_set_ - ipv6, 257
- argv
 - irbe_cli, 51
- as_number
 - irbe_cli::route_origin_elt, 112
 - rpki::left_right::route_origin_elt, 205
- asID
 - rpki::roa::RouteOriginAttestation, 270
- asn
 - rpki::left_right::list_resources_elt, 187
 - rpki::resource_set::resource_bag, 241
- assert_pristine
 - rpki::sql::session, 295
- async.py(2481), 391
- asynchat::async_chat, 96
- asyncore::dispatcher, 97
- attributes
 - rpki::left_right::bsc_elt, 175
 - rpki::left_right::child_elt, 179
 - rpki::left_right::list_resources_elt, 187
 - rpki::left_right::list_roa_requests_ - elt, 189
 - rpki::left_right::parent_elt, 193
 - rpki::left_right::report_error_elt, 197
 - rpki::left_right::repository_elt, 199
 - rpki::left_right::route_origin_elt, 206
 - rpki::left_right::self_elt, 213
 - rpki::publication::client_elt, 223
 - rpki::publication::config_elt, 227
 - rpki::publication::publication_ - object_elt, 235
 - rpki::publication::report_error_elt, 236
 - rpki::xml_utils::base_elt, 380
- b
 - rpki::x509::PEM_converter, 357
- base_uri
 - rpki::publication::client_elt, 223

- bits
 - rpki::ipaddr::v4addr, [171](#)
 - rpki::ipaddr::v6addr, [173](#)
- body
 - rpki::https::http_message, [154](#)
- booleans
 - rpki::left_right::bsc_elt, [175](#)
 - rpki::left_right::child_elt, [179](#)
 - rpki::left_right::parent_elt, [194](#)
 - rpki::left_right::route_origin_elt, [206](#)
 - rpki::left_right::self_elt, [213](#)
 - rpki::xml_utils::base_elt, [380](#)
- bpki_cert
 - irbe_cli::cmd_elt_mixin, [103](#)
 - rpki::left_right::child_elt, [179](#)
 - rpki::left_right::self_elt, [214](#)
 - rpki::publication::client_elt, [223](#)
- bpki_cms_cert
 - irbe_cli::cmd_elt_mixin, [103](#)
 - rpki::left_right::parent_elt, [194](#)
 - rpki::left_right::repository_elt, [199](#)
- bpki_cms_glue
 - irbe_cli::cmd_elt_mixin, [103](#)
 - rpki::left_right::parent_elt, [194](#)
 - rpki::left_right::repository_elt, [199](#)
- bpki_crl
 - irbe_cli::config_elt, [105](#)
- bpki_glue
 - irbe_cli::cmd_elt_mixin, [103](#)
 - rpki::left_right::child_elt, [179](#)
 - rpki::left_right::self_elt, [214](#)
 - rpki::publication::client_elt, [223](#)
- bpki_https_cert
 - irbe_cli::cmd_elt_mixin, [103](#)
 - rpki::left_right::parent_elt, [194](#)
 - rpki::left_right::repository_elt, [200](#)
- bpki_https_glue
 - irbe_cli::cmd_elt_mixin, [103](#)
 - rpki::left_right::parent_elt, [194](#)
 - rpki::left_right::repository_elt, [200](#)
- bpki_ta
 - irdbd, [54](#)
 - pubd::pubd_context, [116](#)
 - rootd, [61](#)
 - rpki::rpki_engine::rpkid_context, [292](#)
- bsc
 - rpki::left_right::data_elt, [182](#)
- bscs
 - rpki::left_right::self_elt, [210](#)
- buffer
 - rpki::https::http_stream, [168](#)
- build
 - rpki::x509::ROA, [361](#)
 - rpki::x509::SignedManifest, [368](#)
- build_https_ta_cache
 - pubd::pubd_context, [115](#)
 - rpki::https, [71](#)
 - rpki::rpki_engine::rpkid_context, [291](#)
- ca
 - rpki::rpki_engine::ca_detail_obj, [272](#)
- ca_cert_uri
 - rpki::rpki_engine::ca_detail_obj, [276](#)
- ca_detail
 - rpki::left_right::route_origin_elt, [202](#)
 - rpki::rpki_engine::child_cert_obj, [284](#)
 - rpki::rpki_engine::revoked_cert_obj, [288](#)
- ca_detail_id
 - rpki::left_right::route_origin_elt, [206](#)
 - rpki::rpki_engine::child_cert_obj, [286](#)
 - rpki::rpki_engine::revoked_cert_obj, [288](#)
- ca_details
 - rpki::rpki_engine::ca_obj, [279](#)
- ca_from_class_name
 - rpki::left_right::child_elt, [178](#)
- ca_id
 - rpki::rpki_engine::ca_detail_obj, [276](#)
- cache
 - rpki::sql::session, [297](#)

- cache_clear
 - rpki::sql::session, 296
- calculate_SKI
 - rpki::x509, 94
- call_daemon
 - irbe_cli, 50
- call_pubd
 - rpki::left_right::repository_elt, 198
- callback
 - rpki::https::http_request, 159
- caller_function
 - rpki::async::iterator, 124
- cancel
 - rpki::async::timer, 126
- cas
 - rpki::left_right::parent_elt, 192
- cert
 - cross_certify, 46
 - rpki::https::http_client, 149
 - rpki::https::http_listener, 152
 - rpki::https::http_queue, 157
 - rpki::left_right::route_origin_elt, 206
 - rpki::rpki_engine::child_cert_obj, 286
 - rpki::up_down::certificate_elt, 316
- cert_url
 - rpki::up_down::certificate_elt, 316
 - rpki::up_down::class_elt, 319
- certs
 - rpki::up_down::class_elt, 319
- cfg
 - irbe_cli, 51
 - irdbd, 54
 - rootd, 61
- cfg_file
 - irbe_cli, 51
 - irdbd, 54
 - pubd, 58
 - rootd, 62
 - rpkid, 96
- characters
 - rpki::xml_utils::sax_handler, 387
- check_allowed_uri
 - rpki::publication::client_elt, 221
- check_for_updates
 - rpki::rpki_engine::ca_obj, 279
- check_response
 - rpki::up_down::base_elt, 313
 - rpki::up_down::error_response_pdu, 323
 - rpki::up_down::issue_response_pdu, 328
- check_valid_rpki
 - rpki::x509::PKCS10, 358
- child
 - cross_certify, 46
 - rpki::rpki_engine::child_cert_obj, 284
- child_bpki_cert
 - rootd, 62
- child_certs
 - rpki::left_right::child_elt, 178
 - rpki::rpki_engine::ca_detail_obj, 272
- child_id
 - rpki::rpki_engine::child_cert_obj, 286
- children
 - rpki::left_right::bsc_elt, 174
 - rpki::left_right::self_elt, 210
- chunk_body
 - rpki::https::http_stream, 165
- chunk_discard_crlf
 - rpki::https::http_stream, 165
- chunk_discard_trailer
 - rpki::https::http_stream, 165
- chunk_handler
 - rpki::https::http_stream, 168
- chunk_header
 - rpki::https::http_stream, 165
- class_name
 - rpki::up_down::class_elt, 319
 - rpki::up_down::issue_pdu, 327
 - rpki::up_down::revoke_pdu, 336
 - rpki::up_down::revoke_syntax, 338
- classes
 - rpki::up_down::class_response_-syntax, 321
- clear
 - rpki::async::timer, 126
 - rpki::x509::DER_object, 350

- clear_https_ta_cache
 - pubd::pubd_context, 115
 - rpki::left_right::child_elt, 180
 - rpki::publication::client_elt, 223
 - rpki::rpki_engine::rpkid_context, 291
- client
 - rpki::https, 72
 - rpki::https::http_queue, 157
- client_cert
 - irbe_cli, 51
- client_getopt
 - irbe_cli::cmd_elt_mixin, 101
- client_handler
 - pubd::pubd_context, 115
- client_key
 - irbe_cli, 51
- client_poll
 - rpki::left_right::self_elt, 210
- client_query_as_number
 - irbe_cli::route_origin_elt, 111
- 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, 102
- client_query_glue
 - irbe_cli::cmd_elt_mixin, 102
- client_query_https_glue
 - irbe_cli::cmd_elt_mixin, 102
- client_query_ipv4
 - irbe_cli::route_origin_elt, 111
- client_query_ipv6
 - irbe_cli::route_origin_elt, 112
- client_query_signing_cert
 - irbe_cli::bsc_elt, 98
- client_query_signing_cert_crl
 - irbe_cli::bsc_elt, 98
- client_queues
 - rpki::https, 72
- client_reply_decode
 - irbe_cli::bsc_elt, 98
 - irbe_cli::cmd_elt_mixin, 102
- client_reply_show
 - irbe_cli::cmd_elt_mixin, 102
- client_ta
 - irbdb, 55
 - rootd, 62
- client_url_regexp
 - pubd::pubd_context, 116
- close
 - rpki::https::http_stream, 166
 - rpki::sql::session, 296
- cmd
 - rpki::https::http_request, 159
- cms_class
 - irbe_cli, 51
- code
 - rpki::https::http_response, 160
- codes
 - rpki::up_down::error_response_pdu, 324
- collect_incoming_data
 - rpki::https::http_stream, 166
- columns
 - rpki::sql::template, 305
- compose_response
 - rootd, 60
- config.py(2452), 391
- config_id
 - rpki::publication::config_elt, 227
- ConfigParser::RawConfigParser, 97
- connect
 - rpki::sql::session, 296
- construct_sia_uri
 - rpki::rpki_engine::ca_obj, 279
- contains
 - rpki::resource_set::resource_set, 250
- content
 - rpki::x509::CMS_object, 342
 - rpki::x509::DER_CMS_object, 349
 - rpki::x509::XML_CMS_object, 376
- content_class
 - rpki::x509::ROA, 361
 - rpki::x509::SignedManifest, 369
- control_handler
 - pubd::pubd_context, 116

- convert_to_seconds
 - rpki::sundial::timedelta, 311
- create
 - rpki::rpki_engine::ca_detail_obj, 272
 - rpki::rpki_engine::ca_obj, 279
 - rpki::x509::PKCS10, 359
- create_ca
 - rpki::x509::PKCS10, 359
- create_top_level
 - rpki::xml_utils::sax_handler, 388
- critical
 - cross_certify, 47
- crl_interval
 - rpki::left_right::self_elt, 214
- crl_uri
 - rpki::rpki_engine::ca_detail_obj, 272
- crl_uri_tail
 - rpki::rpki_engine::ca_detail_obj, 272
- cronjob_handler
 - rpki::rpki_engine::rpkid_context, 291
- cross_certify, 45
 - cert, 46
 - child, 46
 - critical, 47
 - f, 47
 - keypair, 47
 - lifetime, 47
 - make_ext, 46
 - notAfter, 47
 - now, 47
 - output, 47
 - parent, 47
 - serial, 48
 - serial_file, 48
 - usage, 46
 - value, 48
 - x, 48
- cross_certify.py(2433), 391
- cur
 - irdbd, 55
 - rpki::sql::session, 297
- database
 - rpki::sql::session, 297
- datum_type
 - rpki::resource_set::resource_range_as, 245
 - rpki::resource_set::resource_range_ipv4, 247
 - rpki::resource_set::resource_range_ipv6, 248
- db
 - irdbd, 55
 - rpki::sql::session, 298
- debug
 - rpki::https, 72
 - rpki::log, 78
- debug_cms_certs
 - rpki::x509::CMS_object, 342
- debug_tls_certs
 - rpki::https, 72
- decode
 - rpki::x509::DER_CMS_object, 348
 - rpki::x509::XML_CMS_object, 375
- default_http_version
 - rpki::https, 73
- default_section
 - rpki::config::parser, 130
- default_timeout
 - rpki::https, 73
- del_subject_cert
 - rootd, 60
- delete
 - rpki::rpki_engine::ca_detail_obj, 273
 - rpki::rpki_engine::ca_obj, 280
 - rpki::sql::template, 305
- DER
 - rpki::x509::CMS_object, 342
 - rpki::x509::CRL, 347
 - rpki::x509::DER_object, 355
 - rpki::x509::PKCS10, 360
 - rpki::x509::RSA, 364
 - rpki::x509::RSAPublic, 367
 - rpki::x509::X509, 373
- description
 - rpki::up_down::error_response_pdu, 324

- detach
 - rpki::https::http_queue, 156
- difference
 - rpki::resource_set::resource_set, 250
- dirty
 - rpki::sql::session, 298
- done_callback
 - rpki::async::iterator, 124
- dump_inbound_cms
 - rpki::x509::XML_CMS_object, 376
- dump_on_verify_failure
 - rpki::x509::CMS_object, 342
- dump_outbound_cms
 - rpki::x509::XML_CMS_object, 377
- dump_to_disk
 - rpki::x509::XML_CMS_object, 375
- dumpasn1
 - rpki::x509::DER_object, 351
- dynamic_ta
 - rpki::https::http_listener, 152
- e
 - rpki::x509::PEM_converter, 357
- earlier
 - rpki::sundial::datetime, 307
- econtent_oid
 - rpki::x509::CMS_object, 343
 - rpki::x509::ROA, 361
 - rpki::x509::SignedManifest, 369
 - rpki::x509::XML_CMS_object, 377
- ee_uri
 - rpki::left_right::route_origin_elt, 202
- ee_uri_tail
 - rpki::left_right::route_origin_elt, 202
- element_name
 - rpki::left_right::bsc_elt, 175
 - rpki::left_right::child_elt, 180
 - rpki::left_right::list_resources_elt, 187
 - rpki::left_right::list_roa_requests_elt, 189
 - rpki::left_right::parent_elt, 194
 - rpki::left_right::report_error_elt, 197
 - rpki::left_right::repository_elt, 200
 - rpki::left_right::route_origin_elt, 206
 - rpki::left_right::self_elt, 214
 - rpki::publication::certificate_elt, 220
 - rpki::publication::client_elt, 223
 - rpki::publication::config_elt, 227
 - rpki::publication::crl_elt, 229
 - rpki::publication::manifest_elt, 230
 - rpki::publication::report_error_elt, 236
 - rpki::publication::roa_elt, 237
- elements
 - rpki::left_right::bsc_elt, 175
 - rpki::left_right::child_elt, 180
 - rpki::left_right::parent_elt, 195
 - rpki::left_right::repository_elt, 200
 - rpki::left_right::self_elt, 214
 - rpki::publication::client_elt, 223
 - rpki::publication::config_elt, 227
 - rpki::xml_utils::base_elt, 380
- empty
 - rpki::resource_set::resource_bag, 240
 - rpki::x509::DER_object, 351
- enable_trace
 - rpki::log, 78
- encode
 - rpki::x509::DER_CMS_object, 348
 - rpki::x509::XML_CMS_object, 375
- encoding
 - rpki::left_right::cms_msg, 181
 - rpki::publication::cms_msg, 225
 - rpki::up_down::cms_msg, 322
- endElement
 - rpki::left_right::child_elt, 178
 - rpki::publication::client_elt, 221
 - rpki::publication::publication_object_elt, 234
 - rpki::up_down::base_elt, 313
 - rpki::up_down::certificate_elt, 315
 - rpki::up_down::class_elt, 318
 - rpki::up_down::error_response_pdu, 323
 - rpki::up_down::issue_pdu, 326
 - rpki::xml_utils::base_elt, 378
 - rpki::xml_utils::data_elt, 381

- rpki::xml_utils::msg, 385
- rpki::xml_utils::sax_handler, 388
- endElementNS
 - rpki::xml_utils::sax_handler, 388
- enforce_strict_up_down_xml_sender
 - rpki::left_right, 76
- errback
 - rpki::async::timer, 126, 128
 - rpki::https::http_request, 159
- error
 - rpki::log, 78
- error_code
 - rpki::left_right::report_error_elt, 197
 - rpki::publication::report_error_elt, 237
- event_loop
 - rpki::async, 67
- Exception, 97
- exceptions
 - rpki::up_down::error_response_pdu, 324
- exceptions.py(2493), 392
- excludes
 - irbe_cli::bsc_elt, 98
 - irbe_cli::cmd_elt_mixin, 103
- execute
 - rpki::sql::session, 296
- executemany
 - rpki::sql::session, 296
- exit_event_loop
 - rpki::async, 67
- ExitNow
 - rpki::async, 67
- expect_close
 - rpki::https::http_client, 149
 - rpki::https::http_server, 163
- expired
 - rpki::x509::X509, 371
- expires
 - rpki::rpki_engine::revoked_cert_obj, 288
- explicitVersion
 - rpki::manifest::Manifest, 219
 - rpki::roa::RouteOriginAttestation, 270
- extract
 - rpki::x509::CMS_object, 340
- f
 - cross_certify, 47
- fetch
 - rpki::publication::config_elt, 226
 - rpki::rpki_engine::child_cert_obj, 285
- fetch_active
 - rpki::rpki_engine::ca_obj, 280
- fetch_deprecated
 - rpki::rpki_engine::ca_obj, 280
- fetch_pending
 - rpki::rpki_engine::ca_obj, 280
- fetch_revoked
 - rpki::rpki_engine::ca_obj, 280
- fetchall
 - rpki::sql::session, 296
- file
 - rpki::manifest::FileAndHash, 217
- fileHashAlg
 - rpki::manifest::Manifest, 219
- fileList
 - rpki::manifest::Manifest, 219
- find_handler
 - rpki::https::http_server, 162
- format
 - rpki::https::http_message, 153
- format_first_line
 - rpki::https::http_request, 158
 - rpki::https::http_response, 160
- formats
 - rpki::x509::CMS_object, 343
 - rpki::x509::CRL, 347
 - rpki::x509::DER_object, 355
 - rpki::x509::PKCS10, 360
 - rpki::x509::RSA, 364
 - rpki::x509::RSAPublic, 367
 - rpki::x509::X509, 373
- found_terminator
 - rpki::https::http_stream, 166
- from_bytes
 - rpki::ipaddrs::v4addr, 170
 - rpki::ipaddrs::v6addr, 172
- from_exception
 - rpki::left_right::report_error_elt, 196

- rpki::publication::report_error_elt,
236
- from_resource_bag
 - rpki::up_down::class_elt, 318
- from_rfc3779_tuples
 - rpki::resource_set::resource_bag,
240
- from_sql
 - rpki::resource_set::resource_set, 250
 - rpki::resource_set::roa_prefix_set,
262
 - rpki::sundial::datetime, 307
 - rpki::x509::DER_object, 351
- fromASN1tuple
 - rpki::sundial::datetime, 308
- fromdatetime
 - rpki::sundial::datetime, 308
- fromGeneralizedTime
 - rpki::sundial::datetime, 308
- fromtimedelta
 - rpki::sundial::timedelta, 311
- fromUTCTime
 - rpki::sundial::datetime, 308
- fromXMLtime
 - rpki::sundial::datetime, 308
- gAKI
 - rpki::x509::DER_object, 351
- gctx
 - rpki::rpki_engine::ca_detail_obj,
276
 - rpki::rpki_engine::ca_obj, 282
 - rpki::rpki_engine::child_cert_obj,
286
 - rpki::rpki_engine::revoked_cert_obj,
289
 - rpki::sql::sql_persistent, 303
- generate
 - rpki::x509::CRL, 345
 - rpki::x509::RSA, 363
- generate_crl
 - rpki::rpki_engine::ca_detail_obj,
273
- generate_manifest
 - rpki::rpki_engine::ca_detail_obj,
273
- generate_manifest_cert
 - rpki::rpki_engine::ca_detail_obj,
273
- generate_roa
 - rpki::left_right::route_origin_elt,
203
- get
 - rpki::config::parser, 129
- get_3779resources
 - rpki::x509::DER_object, 351
- get_AIA
 - rpki::x509::DER_object, 352
- get_AKI
 - rpki::x509::DER_object, 352
- get_Base64
 - rpki::x509::DER_object, 352
- get_basicConstraints
 - rpki::x509::DER_object, 352
- get_buffer
 - rpki::https::http_stream, 166
- get_content
 - rpki::x509::CMS_object, 341
- get_DER
 - rpki::x509::CMS_object, 341
 - rpki::x509::CRL, 345
 - rpki::x509::DER_object, 352
 - rpki::x509::PKCS10, 359
 - rpki::x509::RSA, 363
 - rpki::x509::RSAPublic, 366
 - rpki::x509::X509, 371
- get_PEM
 - rpki::x509::DER_object, 353
- get_POW
 - rpki::x509::CMS_object, 341
 - rpki::x509::CRL, 345
 - rpki::x509::RSA, 363
 - rpki::x509::RSAPublic, 366
 - rpki::x509::X509, 371
- get_POWpkix
 - rpki::x509::CRL, 346
 - rpki::x509::PKCS10, 359
 - rpki::x509::X509, 371
- get_public_DER
 - rpki::x509::RSA, 363
- get_RSAPublic
 - rpki::x509::RSA, 364

- get_SIA
 - rpki::x509::DER_object, 353
- get_SKI
 - rpki::up_down::revoke_pdu, 335
 - rpki::x509::DER_object, 353
 - rpki::x509::RSA, 364
 - rpki::x509::RSAPublic, 366
- get_subject_cert
 - rootd, 60
- get_subject_pkcs10
 - rootd, 61
- getIssuer
 - rpki::x509::CRL, 346
 - rpki::x509::X509, 371
- getNextUpdate
 - rpki::x509::CRL, 346
 - rpki::x509::SignedManifest, 368
- getNotAfter
 - rpki::x509::X509, 371
- getNotBefore
 - rpki::x509::X509, 372
- getPublicKey
 - rpki::x509::PKCS10, 359
 - rpki::x509::X509, 372
- getSerial
 - rpki::x509::X509, 372
- getSubject
 - rpki::x509::X509, 372
- getThisUpdate
 - rpki::x509::CRL, 346
 - rpki::x509::SignedManifest, 368
- gSKI
 - rpki::x509::DER_object, 353
- hAKI
 - rpki::x509::DER_object, 354
- handle_accept
 - rpki::https::http_listener, 151
- handle_body
 - rpki::https::http_stream, 166
- handle_close
 - rpki::https::http_client, 147
 - rpki::https::http_stream, 166
- handle_connect
 - rpki::https::http_client, 147
- handle_error
 - rpki::https::http_client, 147
 - rpki::https::http_listener, 151
 - rpki::https::http_stream, 166
- handle_message
 - rpki::https::http_client, 148
 - rpki::https::http_server, 162
- handle_no_content_length
 - rpki::https::http_client, 148
 - rpki::https::http_server, 162
- handle_read
 - rpki::https::http_stream, 167
- handle_timeout
 - rpki::https::http_client, 148
 - rpki::https::http_stream, 167
- handle_write
 - rpki::https::http_stream, 167
- handler
 - irdbd, 54
 - rpki::async::timer, 126, 128
- handler_common
 - pubd::pubd_context, 116
- handlers
 - irdbd, 55
 - rootd, 62
 - rpki::https::http_listener, 152
 - rpki::https::http_server, 163
- handles
 - rpki::left_right::bsc_elt, 175
 - rpki::left_right::child_elt, 180
 - rpki::left_right::data_elt, 184
 - rpki::left_right::parent_elt, 195
 - rpki::left_right::repository_elt, 200
 - rpki::left_right::route_origin_elt, 206
 - rpki::left_right::self_elt, 214
- hash
 - rpki::manifest::FileAndHash, 217
- headers
 - rpki::https::http_message, 154
- host
 - irdbd, 55
 - rootd, 62
- hostport
 - rpki::https::http_client, 149
 - rpki::https::http_queue, 157
- hSKI

- rpki::x509::DER_object, 354
- https.py(2493), 393
- https_server_host
 - pubd::pubd_context, 116
 - rootd, 62
 - rpki::rpki_engine::rpkid_context, 292
- https_server_port
 - pubd::pubd_context, 116
 - rootd, 62
 - rpki::rpki_engine::rpkid_context, 293
- https_ta_cache
 - pubd::pubd_context, 117
 - rpki::rpki_engine::rpkid_context, 293
- ignore
 - rpki::async::iterator, 123
- index
 - rpki::sql::template, 305
- info
 - rpki::log, 78
- inherit
 - rpki::resource_set::resource_set, 252
 - rpki::resource_set::resource_set_as, 253
 - rpki::resource_set::resource_set_ip, 255
- inherit_token
 - rpki::resource_set, 86
- init
 - rpki::log, 77
- initate_send
 - rpki::https::http_stream, 167
- insert
 - rpki::sql::template, 305
- intersection
 - rpki::resource_set::resource_bag, 240
 - rpki::resource_set::resource_set, 250
- ipAddrBlocks
 - rpki::roa::RouteOriginAttestation, 270
- ipaddrs.py(2424), 394
- ipv4
 - irbe_cli::route_origin_elt, 112
 - rpki::left_right::list_resources_elt, 187
 - rpki::left_right::list_roa_requests_elt, 189
 - rpki::left_right::route_origin_elt, 207
- ipv6
 - irbe_cli::route_origin_elt, 112
 - rpki::left_right::list_resources_elt, 187
 - rpki::left_right::list_roa_requests_elt, 189
 - rpki::left_right::route_origin_elt, 207
- irbe_cert
 - pubd::pubd_context, 117
 - rpki::rpki_engine::rpkid_context, 293
- irbe_cli, 48
 - argv, 51
 - call_daemon, 50
 - cfg, 51
 - cfg_file, 51
 - client_cert, 51
 - client_key, 51
 - cms_class, 51
 - pem_out, 51
 - q_msg, 51
 - q_msg_left_right, 52
 - q_msg_publication, 52
 - q_pdu, 52
 - server_ta, 52
 - top_opts, 52
 - url, 52
 - usage, 50
 - usage_fill, 52
 - verbose, 53
- irbe_cli.py(2452), 394
- irbe_cli::bsc_elt, 97
 - client_query_signing_cert, 98
 - client_query_signing_cert_crl, 98
 - client_reply_decode, 98
 - excludes, 98
 - signing_cert, 99
 - signing_cert_crl, 99

- irbe_cli::certificate_elt, 99
- irbe_cli::child_elt, 99
- irbe_cli::client_elt, 100
- irbe_cli::cmd_elt_mixin, 100
 - bpki_cert, 103
 - bpki_cms_cert, 103
 - bpki_cms_glue, 103
 - bpki_glue, 103
 - 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, 102
 - client_query_glue, 102
 - client_query_https_glue, 102
 - client_reply_decode, 102
 - client_reply_show, 102
 - excludes, 103
 - usage, 102
- irbe_cli::cmd_msg_mixin, 104
 - usage, 104
- irbe_cli::config_elt, 105
 - bpki_crl, 105
 - client_query_bpki_crl, 105
- irbe_cli::crl_elt, 105
- irbe_cli::left_right_cms_msg, 106
 - saxify, 106
- irbe_cli::left_right_msg, 106
 - pdu, 107
- irbe_cli::left_right_sax_handler, 107
 - pdu, 107
- irbe_cli::manifest_elt, 108
- irbe_cli::parent_elt, 108
- irbe_cli::publication_cms_msg, 108
 - saxify, 109
- irbe_cli::publication_msg, 109
 - pdu, 109
- irbe_cli::publication_sax_handler, 110
 - pdu, 110
- irbe_cli::repository_elt, 110
- irbe_cli::roa_elt, 110
- irbe_cli::route_origin_elt, 111
 - as_number, 112
 - client_query_as_number, 111
 - client_query_ipv4, 111
 - client_query_ipv6, 112
 - ipv4, 112
 - ipv6, 112
- irbe_cli::self_elt, 113
- irbe_cli::UsageWrapper, 113
 - __call__, 113
- irdb_cert
 - rpki::rpki_engine::rpkid_context, 293
- irdb_query
 - rpki::rpki_engine::rpkid_context, 291
- irdb_query_child_resources
 - rpki::rpki_engine::rpkid_context, 291
- irdb_query_roa_requests
 - rpki::rpki_engine::rpkid_context, 292
- irdb_url
 - rpki::rpki_engine::rpkid_context, 293
- irdbd, 53
 - bpki_ta, 54
 - cfg, 54
 - cfg_file, 54
 - client_ta, 55
 - cur, 55
 - db, 55
 - handler, 54
 - handlers, 55
 - host, 55
 - irdbd_cert, 55
 - irdbd_key, 56
 - port, 56
 - rpkid_cert, 56
 - server_cert, 56
 - startup_msg, 56
 - u, 56
- irdbd.py(2502), 396
- irdbd_cert
 - irdbd, 55
- irdbd_key
 - irdbd, 56
- is_CA
 - rpki::x509::DER_object, 354

- is_set
 - rpki::async::timer, 126
- issubset
 - rpki::resource_set::resource_set, 251
- issue
 - rpki::rpki_engine::ca_detail_obj, 273
 - rpki::x509::X509, 372
- issue_ee
 - rpki::rpki_engine::ca_detail_obj, 274
- issue_subject_cert_maybe
 - rootd, 61
- issuer
 - rpki::up_down::class_elt, 319
- issuperset
 - rpki::resource_set::resource_set, 251
- item_callback
 - rpki::async::iterator, 124
- iterator
 - rpki::async::iterator, 124
- key
 - rpki::https::http_client, 149
 - rpki::https::http_listener, 152
 - rpki::https::http_queue, 157
- keypair
 - cross_certify, 47
- last_crl_sn
 - rpki::rpki_engine::ca_obj, 282
- last_issued_sn
 - rpki::rpki_engine::ca_obj, 282
- last_manifest_sn
 - rpki::rpki_engine::ca_obj, 282
- lastrowid
 - rpki::sql::session, 296
- later
 - rpki::sundial::datetime, 309
- latest_ca_cert
 - rpki::rpki_engine::ca_detail_obj, 276
- latest_crl
 - rpki::rpki_engine::ca_detail_obj, 276
- latest_manifest
 - rpki::rpki_engine::ca_detail_obj, 276
- latest_manifest_cert
 - rpki::rpki_engine::ca_detail_obj, 276
- left_right
 - rpki::relaxng, 83
- left_right.py(2504), 396
- left_right_handler
 - rpki::rpki_engine::rpkid_context, 292
- lifetime
 - cross_certify, 47
- log
 - rpki::https::http_listener, 152
 - rpki::https::http_queue, 157
 - rpki::https::http_stream, 168
- log.py(2452), 397
- log_cert
 - rpki::https::http_stream, 167
- logger
 - rpki::https, 72
- long, 114
- looks_like_PEM
 - rpki::x509::PEM_converter, 356
- main
 - pubd, 58
 - rpkid, 96
- make_b64elt
 - rpki::up_down::base_elt, 313
 - rpki::xml_utils::base_elt, 378
- make_elt
 - rpki::up_down::base_elt, 314
 - rpki::xml_utils::base_elt, 379
- make_ext
 - cross_certify, 46
- make_pdu
 - rpki::xml_utils::base_elt, 379
- make_prefix
 - rpki::resource_set::resource_range_ip, 246
- make_query
 - rpki::up_down::message_pdu, 331
- make_reply
 - rpki::xml_utils::data_elt, 382

- make_reply_clone_hook
 - rpki::left_right::data_elt, [182](#)
 - rpki::xml_utils::data_elt, [382](#)
- manifest.py(2424), [398](#)
- manifest_private_key_id
 - rpki::rpki_engine::ca_detail_obj, [276](#)
- manifest_public_key
 - rpki::rpki_engine::ca_detail_obj, [277](#)
- manifest_uri
 - rpki::rpki_engine::ca_detail_obj, [274](#)
- manifestNumber
 - rpki::manifest::Manifest, [219](#)
- map
 - rpki::sql::template, [305](#)
- max
 - rpki::resource_set::resource_range, [243](#)
 - rpki::resource_set::roa_prefix, [259](#)
- max_prefixlen
 - rpki::resource_set::roa_prefix, [260](#)
- maxLength
 - rpki::roa::ROAIPAddress, [266](#)
- min
 - rpki::resource_set::resource_range, [243](#)
 - rpki::resource_set::resource_range_as, [245](#)
 - rpki::resource_set::roa_prefix, [259](#)
- msg
 - rpki::https::http_stream, [169](#)
- multiget
 - rpki::config::parser, [130](#)
- name
 - rpki::left_right::sax_handler, [208](#)
 - rpki::publication::sax_handler, [238](#)
 - rpki::up_down::sax_handler, [338](#)
- name2oid
 - rpki::oids, [80](#)
- name2type
 - rootd::message_pdu, [120](#)
 - rpki::up_down::message_pdu, [332](#)
- next_crl_number
 - rpki::rpki_engine::ca_obj, [281](#)
- next_manifest_number
 - rpki::rpki_engine::ca_obj, [281](#)
- next_serial_number
 - rpki::rpki_engine::ca_obj, [281](#)
- nextUpdate
 - rpki::manifest::Manifest, [219](#)
 - rpki::rpki_engine::ca_detail_obj, [277](#)
- normalize_chain
 - rpki::x509::X509, [373](#)
- normalize_headers
 - rpki::https::http_message, [154](#)
- notAfter
 - cross_certify, [47](#)
- note
 - rpki::log, [78](#)
- now
 - cross_certify, [47](#)
 - rpki::sundial, [90](#)
- nsmap
 - rpki::left_right::left_right_namespace, [185](#)
 - rpki::publication::publication_namespace, [232](#)
 - rpki::up_down, [92](#)
- obj2elt
 - rpki::publication, [83](#)
- object, [114](#)
- oid2name
 - rpki::oids, [80](#)
- oids.py(2424), [398](#)
- other_clear
 - rpki::x509::CMS_object, [343](#)
 - rpki::x509::DER_object, [355](#)
- output
 - cross_certify, [47](#)
- oversized
 - rpki::resource_set::resource_bag, [241](#)
- parent
 - cross_certify, [47](#)
 - rpki::rpki_engine::ca_obj, [281](#)
- parent_id

- rpki::rpki_engine::ca_obj, 282
- parent_resource_class
 - rpki::rpki_engine::ca_obj, 283
- parents
 - rpki::left_right::bsc_elt, 174
 - rpki::left_right::child_elt, 178
 - rpki::left_right::repository_elt, 198
 - rpki::left_right::self_elt, 210
- parse
 - rpki::sundial::timedelta, 311
- parse_first_line
 - rpki::https::http_request, 158
 - rpki::https::http_response, 160
- parse_from_wire
 - rpki::https::http_message, 154
- parse_rfc3779_tuple
 - rpki::resource_set::resource_set_as, 253
 - rpki::resource_set::resource_set_ip, 254
- parse_str
 - rpki::resource_set::resource_set_as, 253
 - rpki::resource_set::resource_set_ip, 254
 - rpki::resource_set::roa_prefix_set, 263
- parse_type
 - rpki::https::http_client, 149
 - rpki::https::http_server, 163
- parse_version
 - rpki::https::http_message, 154
- password
 - rpki::sql::session, 298
- path
 - rpki::https::http_request, 159
- payload
 - rpki::publication::publication_object_elt, 235
 - rpki::up_down::message_pdu, 332
- payload_type
 - rpki::publication::certificate_elt, 220
 - rpki::publication::crl_elt, 229
 - rpki::publication::manifest_elt, 230
 - rpki::publication::roa_elt, 237
- pdu
 - irbe_cli::left_right_sax_handler, 107
 - irbe_cli::publication_sax_handler, 110
 - rootd::sax_handler, 122
 - rpki::left_right::sax_handler, 208
 - rpki::publication::sax_handler, 238
 - rpki::up_down::sax_handler, 339
- pdu
 - irbe_cli::left_right_msg, 107
 - irbe_cli::publication_msg, 109
 - rpki::left_right::msg, 190
 - rpki::publication::msg, 231
- pem_converter
 - rpki::x509::CMS_object, 343
 - rpki::x509::CRL, 347
 - rpki::x509::DER_object, 355
 - rpki::x509::PKCS10, 360
 - rpki::x509::ROA, 362
 - rpki::x509::RSA, 364
 - rpki::x509::RSAPublic, 367
 - rpki::x509::SignedManifest, 369
 - rpki::x509::X509, 373
- pem_out
 - irbe_cli, 51
- persistent
 - rpki::https::http_message, 154
- pid
 - rpki::log, 78
- ping
 - rpki::sql::session, 297
- pkcs10
 - rpki::up_down::issue_pdu, 327
- pkcs10_request
 - rpki::left_right::bsc_elt, 175
- PKIX_threshold
 - rpki::sundial::datetime, 310
- port
 - irdbd, 56
 - rootd, 63
- POW
 - rpki::x509::CMS_object, 344
 - rpki::x509::CRL, 347
 - rpki::x509::RSA, 365
 - rpki::x509::RSAPublic, 367
 - rpki::x509::X509, 374
- POWify_OID

- rpki::x509, 94
- POWpkix
 - rpki::x509::CRL, 347
 - rpki::x509::PKCS10, 360
 - rpki::x509::X509, 374
- prefix_type
 - rpki::resource_set::roa_prefix_set-ipv4, 264
 - rpki::resource_set::roa_prefix_set-ipv6, 265
- prefixlen
 - rpki::resource_set::roa_prefix, 260
- pretty_print_content
 - rpki::x509::XML_CMS_object, 375
- print_on_der_error
 - rpki::x509::CMS_object, 344
- priority
 - rpki::log::logger, 216
- private_key_id
 - rpki::left_right::bsc_elt, 176
 - rpki::rpki_engine::ca_detail_obj, 277
- profile
 - pubd, 58
 - rpkid, 96
- pubd, 57
 - cfg_file, 58
 - main, 58
 - profile, 58
- pubd.py(2493), 399
- 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, 277
 - publication
 - rpki::relaxng, 83
 - publication.py(2493), 399
 - publication_base
 - pubd::pubd_context, 117
 - publication_kludge_base
 - rpki::rpki_engine::rpkid_context, 293
 - publish
 - rpki::left_right::repository_elt, 199
 - publish_ee_separately
 - rpki::left_right::route_origin_elt, 207
 - pydatetime::datetime, 118
 - pydatetime::timedelta, 118
- q_msg
 - irbe_cli, 51
- q_msg_left_right
 - irbe_cli, 52
- q_msg_publication
 - irbe_cli, 52
- q_pdu
 - irbe_cli, 52
- query
 - rpki::up_down::issue_pdu, 326
 - rpki::up_down::list_pdu, 329
 - rpki::up_down::revoke_pdu, 335
- query_up_down
 - rpki::left_right::parent_elt, 192
- queue
 - rpki::async::timer, 128
 - rpki::https::http_client, 149
 - rpki::https::http_queue, 157
- range_type
 - rpki::resource_set::resource_set_as, 253

- rpki::resource_set::resource_set_
 ipv4, 256
- rpki::resource_set::resource_set_
 ipv6, 257
- rpki::resource_set::roa_prefix_ipv4,
 261
- rpki::resource_set::roa_prefix_ipv6,
 261
- read_attrs
 - rpki::xml_utils::base_elt, 379
- readable
 - rpki::https::http_stream, 167
- reason
 - rpki::https::http_response, 160
- recipient
 - rpki::up_down::message_pdu, 332
- recv
 - rpki::https::http_stream, 167
- regen_margin
 - rpki::left_right::self_elt, 215
- regenerate_crls_and_manifests
 - rpki::left_right::self_elt, 211
- regenerate_roa
 - rpki::left_right::route_origin_elt,
 203
- regex
 - rpki::sundial::timedelta, 312
- reissue
 - rpki::rpki_engine::child_cert_obj,
 285
- rekey
 - rpki::rpki_engine::ca_obj, 281
- relaxng.py(2501), 400
- repositories
 - rpki::left_right::bsc_elt, 174
 - rpki::left_right::self_elt, 211
- repository
 - rpki::left_right::parent_elt, 192
- req_resource_set_as
 - rpki::up_down::certificate_elt, 316
 - rpki::up_down::issue_pdu, 327
- req_resource_set_ipv4
 - rpki::up_down::certificate_elt, 316
 - rpki::up_down::issue_pdu, 327
- req_resource_set_ipv6
 - rpki::up_down::certificate_elt, 316
- rpki::up_down::issue_pdu, 327
- request
 - rpki::https::http_queue, 156
- require_crls
 - rpki::x509::CMS_object, 344
- resource_set.py(2457), 400
- resource_set_as
 - rpki::up_down::class_elt, 319
- resource_set_ipv4
 - rpki::up_down::class_elt, 319
- resource_set_ipv6
 - rpki::up_down::class_elt, 319
- resource_set_notafter
 - rpki::up_down::class_elt, 320
- resource_set_type
 - rpki::resource_set::roa_prefix_set_
 ipv4, 264
 - rpki::resource_set::roa_prefix_set_
 ipv6, 265
- restart
 - rpki::https::http_queue, 156
 - rpki::https::http_stream, 168
- result
 - rpki::xml_utils::sax_handler, 389
- retrieved
 - rpki::https::http_request, 159
- retry_read
 - rpki::https::http_client, 149
 - rpki::https::http_server, 163
 - rpki::https::http_stream, 169
- retry_write
 - rpki::https::http_client, 150
 - rpki::https::http_server, 163
 - rpki::https::http_stream, 169
- return_result
 - rpki::https::http_queue, 156
- revoke
 - rpki::rpki_engine::ca_detail_obj,
 274
 - rpki::rpki_engine::ca_obj, 282
 - rpki::rpki_engine::child_cert_obj,
 285
 - rpki::rpki_engine::revoked_cert_obj,
 288
- revoked

- rpki::rpki_engine::revoked_cert_obj, 289
- revoked_certs
 - rpki::rpki_engine::ca_detail_obj, 275
- roa
 - rpki::left_right::route_origin_elt, 207
- roa.py(2424), 401
- roa_uri
 - rpki::left_right::route_origin_elt, 203
- roa_uri_tail
 - rpki::left_right::route_origin_elt, 203
- rootd, 58
 - bpki_ta, 61
 - cfg, 61
 - cfg_file, 62
 - child_bpki_cert, 62
 - client_ta, 62
 - compose_response, 60
 - del_subject_cert, 60
 - get_subject_cert, 60
 - get_subject_pkcs10, 61
 - handlers, 62
 - host, 62
 - https_server_host, 62
 - https_server_port, 62
 - issue_subject_cert_maybe, 61
 - port, 63
 - rootd_bpki_cert, 63
 - rootd_bpki_crl, 63
 - rootd_bpki_key, 63
 - rpki_base_uri, 63
 - rpki_class_name, 63
 - rpki_root_cert, 63
 - rpki_root_cert_uri, 64
 - rpki_root_crl, 64
 - rpki_root_dir, 64
 - rpki_root_key, 64
 - rpki_root_manifest, 64
 - rpki_subject_cert, 64
 - rpki_subject_lifetime, 65
 - rpki_subject_pkcs10, 65
 - rpki_subject_regen, 65
 - server_cert, 65
 - set_subject_cert, 61
 - set_subject_pkcs10, 61
 - up_down_handler, 61
- rootd.py(2481), 402
- rootd::cms_msg, 118
 - saxify, 118
- rootd::issue_pdu, 119
 - serve_pdu, 119
- rootd::list_pdu, 119
 - serve_pdu, 120
- rootd::message_pdu, 120
 - name2type, 120
 - type2name, 121
- rootd::revoke_pdu, 121
 - serve_pdu, 121
- rootd::sax_handler, 122
 - pdu, 122
- rootd_bpki_cert
 - rootd, 63
- rootd_bpki_crl
 - rootd, 63
- rootd_bpki_key
 - rootd, 63
- route_origins
 - rpki::left_right::self_elt, 211
 - rpki::rpki_engine::ca_detail_obj, 275
- rpki, 65
 - rpki.async, 66
 - rpki.config, 67
 - rpki.exceptions, 68
 - rpki.https, 70
 - rpki.ipaddrs, 73
 - rpki.left_right, 74
 - rpki.log, 76
 - rpki.manifest, 79
 - rpki.oids, 80
 - rpki.publication, 81
 - rpki.relaxng, 83
 - rpki.resource_set, 84
 - rpki.roa, 86
 - rpki.rpki_engine, 88
 - rpki.sql, 88
 - rpki.sundial, 89
 - rpki.up_down, 91

- rpki.x509, [92](#)
- rpki.xml_utils, [94](#)
- rpki::async
 - _raiseExitNow, [67](#)
 - event_loop, [67](#)
 - exit_event_loop, [67](#)
 - ExitNow, [67](#)
- rpki::async::iterator, [122](#)
 - __call__, [123](#)
 - __init__, [123](#)
 - __repr__, [123](#)
 - caller_function, [124](#)
 - done_callback, [124](#)
 - ignore, [123](#)
 - item_callback, [124](#)
 - iterator, [124](#)
- rpki::async::timer, [124](#)
 - __cmp__, [125](#)
 - __init__, [125](#)
 - __repr__, [126](#)
 - cancel, [126](#)
 - clear, [126](#)
 - errback, [126](#), [128](#)
 - handler, [126](#), [128](#)
 - is_set, [126](#)
 - queue, [128](#)
 - runq, [127](#)
 - seconds_until_wakeup, [127](#)
 - set, [127](#)
 - set_errback, [127](#)
 - set_handler, [128](#)
 - when, [128](#)
- rpki::config::parser, [129](#)
 - __init__, [129](#)
 - default_section, [130](#)
 - get, [129](#)
 - multiget, [130](#)
- rpki::exceptions::BadClassNameSyntax, [130](#)
- rpki::exceptions::BadClientURL, [131](#)
- rpki::exceptions::BadContactURL, [131](#)
- rpki::exceptions::BadExtension, [131](#)
- rpki::exceptions::BadIRDBReply, [132](#)
- rpki::exceptions::BadIssueResponse, [132](#)
- rpki::exceptions::BadPKCS10, [132](#)
- rpki::exceptions::BadPublicationReply, [133](#)
- rpki::exceptions::BadQuery, [133](#)
- rpki::exceptions::BadSender, [133](#)
- rpki::exceptions::BadStatusCode, [134](#)
- rpki::exceptions::BadURISyntax, [134](#)
- rpki::exceptions::BSCNotFound, [134](#)
- rpki::exceptions::ChildNotFound, [135](#)
- rpki::exceptions::ClassNameMismatch, [135](#)
- rpki::exceptions::ClassNameUnknown, [135](#)
- rpki::exceptions::ClientNotFound, [136](#)
- rpki::exceptions::CMSCRLNotSet, [136](#)
- rpki::exceptions::CMSVerificationFailed, [136](#)
- rpki::exceptions::DBConsistencyError, [137](#)
- rpki::exceptions::DERObjectConversionError, [137](#)
- rpki::exceptions::DuplicateObject, [137](#)
- rpki::exceptions::EmptyPEM, [138](#)
- rpki::exceptions::ForbiddenURI, [138](#)
- rpki::exceptions::HTTPRequestFailed, [138](#)
- rpki::exceptions::HTTPSClientAborted, [139](#)
- rpki::exceptions::MissingCMSCRL, [139](#)
- rpki::exceptions::MissingCMSEECert, [139](#)
- rpki::exceptions::MultipleTLSEECert, [140](#)
- rpki::exceptions::MustBePrefix, [140](#)
- rpki::exceptions::NoActiveCA, [140](#)
- rpki::exceptions::NotACertificateChain, [141](#)
- rpki::exceptions::NotFound, [141](#)
- rpki::exceptions::NotImplementedYet, [141](#)
- rpki::exceptions::NotInDatabase, [142](#)
- rpki::exceptions::ReceivedTLSCACert, [142](#)
- rpki::exceptions::RPKI_Exception, [142](#)
- rpki::exceptions::ServerShuttingDown, [143](#)
- rpki::exceptions::SKIMismatch, [143](#)

- rpki::exceptions::SubprocessError, [144](#)
- rpki::exceptions::TLSValidationError, [144](#)
- rpki::exceptions::UnexpectedCMSCerts, [144](#)
- rpki::exceptions::UnexpectedCMSCRLs, [145](#)
- rpki::exceptions::UnparsableCMSDER, [145](#)
- rpki::exceptions::UpstreamError, [145](#)
- rpki::exceptions::WrongEContentType, [146](#)
- rpki::https
 - build_https_ta_cache, [71](#)
 - client, [72](#)
 - client_queues, [72](#)
 - debug, [72](#)
 - debug_tls_certs, [72](#)
 - default_http_version, [73](#)
 - default_timeout, [73](#)
 - logger, [72](#)
 - rpki_content_type, [73](#)
 - server, [72](#)
 - want_persistent_client, [73](#)
 - want_persistent_server, [73](#)
- rpki::https::http_client, [146](#)
 - __init__, [147](#)
 - cert, [149](#)
 - expect_close, [149](#)
 - handle_close, [147](#)
 - handle_connect, [147](#)
 - handle_error, [147](#)
 - handle_message, [148](#)
 - handle_no_content_length, [148](#)
 - handle_timeout, [148](#)
 - hostport, [149](#)
 - key, [149](#)
 - parse_type, [149](#)
 - queue, [149](#)
 - retry_read, [149](#)
 - retry_write, [150](#)
 - send_request, [148](#)
 - set_state, [148](#)
 - start, [148](#)
 - state, [150](#)
 - ta, [150](#)
 - tls, [150](#)
 - tls_connect, [148](#)
- rpki::https::http_listener, [150](#)
 - __init__, [151](#)
 - cert, [152](#)
 - dynamic_ta, [152](#)
 - handle_accept, [151](#)
 - handle_error, [151](#)
 - handlers, [152](#)
 - key, [152](#)
 - log, [152](#)
 - ta, [152](#)
- rpki::https::http_message, [152](#)
 - __init__, [153](#)
 - __str__, [153](#)
 - body, [154](#)
 - format, [153](#)
 - headers, [154](#)
 - normalize_headers, [154](#)
 - parse_from_wire, [154](#)
 - parse_version, [154](#)
 - persistent, [154](#)
 - software_name, [154](#)
 - version, [155](#)
- rpki::https::http_queue, [155](#)
 - __init__, [156](#)
 - cert, [157](#)
 - client, [157](#)
 - detach, [156](#)
 - hostport, [157](#)
 - key, [157](#)
 - log, [157](#)
 - queue, [157](#)
 - request, [156](#)
 - restart, [156](#)
 - return_result, [156](#)
 - send_request, [156](#)
 - ta, [157](#)
- rpki::https::http_request, [158](#)
 - __init__, [158](#)
 - callback, [159](#)
 - cmd, [159](#)
 - errback, [159](#)
 - format_first_line, [158](#)
 - parse_first_line, [158](#)
 - path, [159](#)

- retried, 159
- rpki::https::http_response, 159
 - __init__, 160
 - code, 160
 - format_first_line, 160
 - parse_first_line, 160
 - reason, 160
- rpki::https::http_server, 161
 - __init__, 162
 - expect_close, 163
 - find_handler, 162
 - handle_message, 162
 - handle_no_content_length, 162
 - handlers, 163
 - parse_type, 163
 - retry_read, 163
 - retry_write, 163
 - send_error, 162
 - send_message, 162
 - send_reply, 162
 - tls, 164
 - tls_accept, 163
- rpki::https::http_stream, 164
 - __init__, 165
 - buffer, 168
 - chunk_body, 165
 - chunk_discard_crlf, 165
 - chunk_discard_trailer, 165
 - chunk_handler, 168
 - chunk_header, 165
 - close, 166
 - collect_incoming_data, 166
 - found_terminator, 166
 - get_buffer, 166
 - handle_body, 166
 - handle_close, 166
 - handle_error, 166
 - handle_read, 167
 - handle_timeout, 167
 - handle_write, 167
 - initiate_send, 167
 - log, 168
 - log_cert, 167
 - msg, 169
 - readable, 167
 - recv, 167
 - restart, 168
 - retry_read, 169
 - retry_write, 169
 - send, 168
 - timeout, 169
 - timer, 169
 - tls, 169
 - update_timeout, 168
 - writeable, 168
- rpki::ipaddr::v4addr, 170
 - __new__, 170
 - __str__, 170
 - bits, 171
 - from_bytes, 170
 - to_bytes, 171
- rpki::ipaddr::v6addr, 171
 - __new__, 172
 - __str__, 172
 - bits, 173
 - from_bytes, 172
 - to_bytes, 172
- rpki::left_right
 - enforce_strict_up_down_xml_sender, 76
- rpki::left_right::bsc_elt, 173
 - attributes, 175
 - booleans, 175
 - children, 174
 - element_name, 175
 - elements, 175
 - handles, 175
 - parents, 174
 - pkcs10_request, 175
 - private_key_id, 176
 - repositories, 174
 - serve_pre_save_hook, 174
 - signing_cert, 176
 - signing_cert_crl, 176
 - sql_template, 176
- rpki::left_right::child_elt, 177
 - attributes, 179
 - booleans, 179
 - bpki_cert, 179
 - bpki_glue, 179
 - ca_from_class_name, 178
 - child_certs, 178

- clear_https_ta_cache, 180
- element_name, 180
- elements, 180
- endElement, 178
- handles, 180
- parents, 178
- serve_post_save_hook, 178
- serve_up_down, 179
- sql_template, 180
- rpki::left_right::cms_msg, 181
 - encoding, 181
 - saxify, 181
 - schema, 181
- rpki::left_right::data_elt, 182
 - bsc, 182
 - handles, 184
 - make_reply_clone_hook, 182
 - self, 183
 - self_id, 184
 - serve_fetch_all, 183
 - serve_fetch_handle, 183
 - serve_fetch_one_maybe, 183
 - serve_pre_save_hook, 184
 - unimplemented_control, 184
- rpki::left_right::left_right_namespace, 185
 - nsmap, 185
 - xmlns, 185
- rpki::left_right::list_resources_elt, 186
 - asn, 187
 - attributes, 187
 - element_name, 187
 - ipv4, 187
 - ipv6, 187
 - startElement, 186
 - toXML, 186
 - valid_until, 188
- rpki::left_right::list_roa_requests_elt, 188
 - attributes, 189
 - element_name, 189
 - ipv4, 189
 - ipv6, 189
 - startElement, 189
- rpki::left_right::msg, 190
 - pdus, 190
 - serve_top_level, 190
 - version, 191
- rpki::left_right::parent_elt, 191
 - attributes, 193
 - booleans, 194
 - bpki_cms_cert, 194
 - bpki_cms_glue, 194
 - bpki_https_cert, 194
 - bpki_https_glue, 194
 - cas, 192
 - element_name, 194
 - elements, 195
 - handles, 195
 - query_up_down, 192
 - repository, 192
 - serve_post_save_hook, 193
 - serve_rekey, 193
 - serve_revoke, 193
 - sql_template, 195
- rpki::left_right::report_error_elt, 196
 - attributes, 197
 - element_name, 197
 - error_code, 197
 - from_exception, 196
 - self_handle, 197
 - text, 197
- rpki::left_right::repository_elt, 197
 - attributes, 199
 - bpki_cms_cert, 199
 - bpki_cms_glue, 199
 - bpki_https_cert, 200
 - bpki_https_glue, 200
 - call_pubd, 198
 - element_name, 200
 - elements, 200
 - handles, 200
 - parents, 198
 - publish, 199
 - sql_template, 200
 - withdraw, 199
- rpki::left_right::route_origin_elt, 201
 - as_number, 205
 - attributes, 206
 - booleans, 206
 - ca_detail, 202
 - ca_detail_id, 206
 - cert, 206

- ee_uri, 202
- ee_uri_tail, 202
- element_name, 206
- generate_roa, 203
- handles, 206
- ipv4, 207
- ipv6, 207
- publish_ee_separately, 207
- regenerate_roa, 203
- roa, 207
- roa_uri, 203
- roa_uri_tail, 203
- serve_post_save_hook, 204
- sql_delete_hook, 204
- sql_fetch_hook, 204
- sql_insert_hook, 204
- sql_template, 207
- startElement, 205
- update_roa, 205
- withdraw_roa, 205
- rpki::left_right::sax_handler, 208
 - name, 208
 - pdu, 208
 - version, 208
- rpki::left_right::self_elt, 209
 - attributes, 213
 - booleans, 213
 - bpki_cert, 214
 - bpki_glue, 214
 - bscs, 210
 - children, 210
 - client_poll, 210
 - crl_interval, 214
 - element_name, 214
 - elements, 214
 - handles, 214
 - parents, 210
 - regen_margin, 215
 - regenerate_crls_and_manifests, 211
 - repositories, 211
 - route_origins, 211
 - serve_fetch_all, 211
 - serve_fetch_handle, 212
 - serve_fetch_one_maybe, 212
 - serve_post_save_hook, 212
 - serve_rekey, 212
 - serve_revoke, 213
 - sql_template, 215
 - update_children, 213
 - update_roas, 213
 - use_hsm, 215
- rpki::log
 - debug, 78
 - enable_trace, 78
 - error, 78
 - info, 78
 - init, 77
 - note, 78
 - pid, 78
 - set_trace, 77
 - tag, 78
 - trace, 77
 - use_syslog, 79
 - warn, 79
- rpki::log::logger, 215
 - __call__, 216
 - __init__, 216
 - priority, 216
- rpki::manifest::FileAndHash, 216
 - __init__, 217
 - file, 217
 - hash, 217
- rpki::manifest::FilesAndHashes, 217
 - __init__, 218
- rpki::manifest::Manifest, 218
 - __init__, 219
 - explicitVersion, 219
 - fileHashAlg, 219
 - fileList, 219
 - manifestNumber, 219
 - nextUpdate, 219
 - thisUpdate, 219
 - version, 219
- rpki::oids
 - name2oid, 80
 - oid2name, 80
- rpki::publication
 - obj2elt, 83
- rpki::publication::certificate_elt, 220
 - element_name, 220
 - payload_type, 220
- rpki::publication::client_elt, 221

- attributes, 223
- base_uri, 223
- bpki_cert, 223
- bpki_glue, 223
- check_allowed_uri, 221
- clear_https_ta_cache, 223
- element_name, 223
- elements, 223
- endElement, 221
- serve_fetch_all, 222
- serve_fetch_one_maybe, 222
- serve_post_save_hook, 222
- sql_template, 224
- rpki::publication::cms_msg, 224
 - encoding, 225
 - saxify, 225
 - schema, 225
- rpki::publication::config_elt, 225
 - attributes, 227
 - config_id, 227
 - element_name, 227
 - elements, 227
 - fetch, 226
 - serve_fetch_one_maybe, 226
 - serve_set, 226
 - sql_template, 228
 - startElement, 227
 - wired_in_config_id, 228
- rpki::publication::control_elt, 228
 - serve_dispatch, 229
- rpki::publication::crl_elt, 229
 - element_name, 229
 - payload_type, 229
- rpki::publication::manifest_elt, 230
 - element_name, 230
 - payload_type, 230
- rpki::publication::msg, 231
 - pdus, 231
 - serve_top_level, 231
 - version, 232
- rpki::publication::publication_namespace, 232
 - nsmap, 232
 - xmlns, 233
- rpki::publication::publication_object_elt, 233
 - attributes, 235
 - endElement, 234
 - payload, 235
 - serve_dispatch, 234
 - serve_publish, 234
 - serve_withdraw, 234
 - toXML, 234
 - uri_to_filename, 235
- rpki::publication::report_error_elt, 235
 - attributes, 236
 - element_name, 236
 - error_code, 237
 - from_exception, 236
- rpki::publication::roa_elt, 237
 - element_name, 237
 - payload_type, 237
- rpki::publication::sax_handler, 238
 - name, 238
 - pdu, 238
 - version, 238
- rpki::relaxng
 - left_right, 83
 - publication, 83
 - up_down, 83
- rpki::resource_set
 - _bs2long, 85
 - _long2bs, 85
 - _rsplit, 86
 - inherit_token, 86
 - test1, 86
 - test2, 86
- rpki::resource_set::resource_bag, 239
 - __eq__, 240
 - __init__, 240
 - __ne__, 240
 - __str__, 240
 - asn, 241
 - empty, 240
 - from_rfc3779_tuples, 240
 - intersection, 240
 - oversized, 241
 - undersized, 241
 - union, 241
 - v4, 241
 - v6, 242
 - valid_until, 242

- rpki::resource_set::resource_range, 242
 - __cmp__, 243
 - __init__, 243
 - max, 243
 - min, 243
- rpki::resource_set::resource_range_as, 244
 - __str__, 244
 - datum_type, 245
 - min, 245
 - to_rfc3779_tuple, 244
- rpki::resource_set::resource_range_ip, 245
 - __str__, 246
 - _prefixlen, 246
 - make_prefix, 246
 - to_rfc3779_tuple, 246
- rpki::resource_set::resource_range_ipv4, 247
 - datum_type, 247
- rpki::resource_set::resource_range_ipv6, 248
 - datum_type, 248
- rpki::resource_set::resource_set, 248
 - __init__, 249
 - __str__, 249
 - _comm, 249
 - contains, 250
 - difference, 250
 - from_sql, 250
 - inherit, 252
 - intersection, 250
 - issubset, 251
 - issuperset, 251
 - symmetric_difference, 251
 - union, 251
- rpki::resource_set::resource_set_as, 252
 - inherit, 253
 - parse_rfc3779_tuple, 253
 - parse_str, 253
 - range_type, 253
 - to_rfc3779_tuple, 253
- rpki::resource_set::resource_set_ip, 254
 - inherit, 255
 - parse_rfc3779_tuple, 254
 - parse_str, 254
 - to_rfc3779_tuple, 255
- rpki::resource_set::resource_set_ipv4, 255
 - afi, 256
 - range_type, 256
- rpki::resource_set::resource_set_ipv6, 256
 - afi, 257
 - range_type, 257
- rpki::resource_set::roa_prefix, 257
 - __cmp__, 258
 - __init__, 258
 - __str__, 258
 - address, 260
 - max, 259
 - max_prefixlen, 260
 - min, 259
 - prefixlen, 260
 - to_resource_range, 259
 - to_roa_tuple, 259
- rpki::resource_set::roa_prefix_ipv4, 260
 - range_type, 261
- rpki::resource_set::roa_prefix_ipv6, 261
 - range_type, 261
- rpki::resource_set::roa_prefix_set, 262
 - __init__, 262
 - __str__, 262
 - from_sql, 262
 - parse_str, 263
 - to_resource_set, 263
 - to_roa_tuple, 263
- rpki::resource_set::roa_prefix_set_ipv4, 264
 - prefix_type, 264
 - resource_set_type, 264
- rpki::resource_set::roa_prefix_set_ipv6, 265
 - prefix_type, 265
 - resource_set_type, 265
- rpki::roa::ROAIPAddress, 266
 - __init__, 266
 - address, 266
 - maxLength, 266
- rpki::roa::ROAIPAddresses, 267
 - __init__, 267
- rpki::roa::ROAIPAddressFamilies, 267

- [__init__, 268](#)
- [rpki::roa::ROAIPAddressFamily, 268](#)
 - [__init__, 268](#)
 - [addresses, 269](#)
 - [addressFamily, 269](#)
- [rpki::roa::RouteOriginAttestation, 269](#)
 - [__init__, 269](#)
 - [asID, 270](#)
 - [explicitVersion, 270](#)
 - [ipAddrBlocks, 270](#)
 - [version, 270](#)
- [rpki::rpki_engine::ca_detail_obj, 270](#)
 - [activate, 272](#)
 - [ca, 272](#)
 - [ca_cert_uri, 276](#)
 - [ca_id, 276](#)
 - [child_certs, 272](#)
 - [create, 272](#)
 - [crl_uri, 272](#)
 - [crl_uri_tail, 272](#)
 - [delete, 273](#)
 - [gctx, 276](#)
 - [generate_crl, 273](#)
 - [generate_manifest, 273](#)
 - [generate_manifest_cert, 273](#)
 - [issue, 273](#)
 - [issue_ee, 274](#)
 - [latest_ca_cert, 276](#)
 - [latest_crl, 276](#)
 - [latest_manifest, 276](#)
 - [latest_manifest_cert, 276](#)
 - [manifest_private_key_id, 276](#)
 - [manifest_public_key, 277](#)
 - [manifest_uri, 274](#)
 - [nextUpdate, 277](#)
 - [private_key_id, 277](#)
 - [public_key, 277](#)
 - [revoke, 274](#)
 - [revoked_certs, 275](#)
 - [route_origins, 275](#)
 - [sql_decode, 275](#)
 - [sql_template, 277](#)
 - [state, 278](#)
 - [update, 275](#)
- [rpki::rpki_engine::ca_obj, 278](#)
 - [ca_details, 279](#)
 - [check_for_updates, 279](#)
 - [construct_sia_uri, 279](#)
 - [create, 279](#)
 - [delete, 280](#)
 - [fetch_active, 280](#)
 - [fetch_deprecated, 280](#)
 - [fetch_pending, 280](#)
 - [fetch_revoked, 280](#)
 - [gctx, 282](#)
 - [last_crl_sn, 282](#)
 - [last_issued_sn, 282](#)
 - [last_manifest_sn, 282](#)
 - [next_crl_number, 281](#)
 - [next_manifest_number, 281](#)
 - [next_serial_number, 281](#)
 - [parent, 281](#)
 - [parent_id, 282](#)
 - [parent_resource_class, 283](#)
 - [rekey, 281](#)
 - [revoke, 282](#)
 - [sia_uri, 283](#)
 - [sql_template, 283](#)
- [rpki::rpki_engine::child_cert_obj, 283](#)
 - [__init__, 284](#)
 - [ca_detail, 284](#)
 - [ca_detail_id, 286](#)
 - [cert, 286](#)
 - [child, 284](#)
 - [child_id, 286](#)
 - [fetch, 285](#)
 - [gctx, 286](#)
 - [reissue, 285](#)
 - [revoke, 285](#)
 - [sql_template, 286](#)
 - [uri, 285](#)
 - [uri_tail, 286](#)
- [rpki::rpki_engine::revoked_cert_obj, 287](#)
 - [__init__, 288](#)
 - [ca_detail, 288](#)
 - [ca_detail_id, 288](#)
 - [expires, 288](#)
 - [gctx, 289](#)
 - [revoke, 288](#)
 - [revoked, 289](#)
 - [serial, 289](#)
 - [sql_template, 289](#)

- rpki::rpki_engine::rpkid_context, 290
 - __init__, 291
 - bpki_ta, 292
 - build_https_ta_cache, 291
 - clear_https_ta_cache, 291
 - cronjob_handler, 291
 - https_server_host, 292
 - https_server_port, 293
 - https_ta_cache, 293
 - irbe_cert, 293
 - irdb_cert, 293
 - irdb_query, 291
 - irdb_query_child_resources, 291
 - irdb_query_roa_requests, 292
 - irdb_url, 293
 - left_right_handler, 292
 - publication_kludge_base, 293
 - rpkid_cert, 293
 - rpkid_key, 294
 - sql, 294
 - up_down_handler, 292
 - up_down_url_regexp, 294
- rpki::sql::session, 294
 - __init__, 295
 - _exceptions_enabled, 297
 - _wrap_execute, 295
 - assert_pristine, 295
 - cache, 297
 - cache_clear, 296
 - close, 296
 - connect, 296
 - cur, 297
 - database, 297
 - db, 298
 - dirty, 298
 - execute, 296
 - executemany, 296
 - fetchall, 296
 - lastrowid, 296
 - password, 298
 - ping, 297
 - sweep, 297
 - username, 298
- rpki::sql::sql_persistent, 298
 - gctx, 303
 - sql_debug, 303
 - sql_decode, 299
 - sql_delete, 300
 - sql_delete_hook, 300
 - sql_deleted, 303
 - sql_encode, 300
 - sql_fetch, 300
 - sql_fetch_all, 301
 - sql_fetch_hook, 301
 - sql_fetch_where, 301
 - sql_fetch_where1, 301
 - sql_in_db, 304
 - sql_init, 301
 - sql_insert_hook, 302
 - sql_is_dirty, 302
 - sql_mark_clean, 302
 - sql_mark_deleted, 302
 - sql_mark_dirty, 302
 - sql_store, 303
 - sql_update_hook, 303
- rpki::sql::template, 304
 - __init__, 305
 - columns, 305
 - delete, 305
 - index, 305
 - insert, 305
 - map, 305
 - select, 305
 - table, 306
 - update, 306
- rpki::sundial
 - now, 90
 - test, 90
- rpki::sundial::datetime, 306
 - __add__, 307
 - __str__, 307
 - __sub__, 307
 - earlier, 307
 - from_sql, 307
 - fromASN1tuple, 308
 - fromdatetime, 308
 - fromGeneralizedTime, 308
 - fromUTCtime, 308
 - fromXMLtime, 308
 - later, 309
 - PKIX_threshold, 310
 - to_sql, 309

- toASN1tuple, 309
- toGeneralizedTime, 309
- totimestamp, 309
- toUTCTime, 310
- toXMLtime, 310
- rpki::sundial::timedelta, 310
 - convert_to_seconds, 311
 - fromtimedelta, 311
 - parse, 311
 - regexp, 312
- rpki::up_down
 - nsmmap, 92
 - xmlns, 92
- rpki::up_down::base_elt, 312
 - check_response, 313
 - endElement, 313
 - make_b64elt, 313
 - make_elt, 314
 - serve_pdu, 314
 - startElement, 314
- rpki::up_down::certificate_elt, 315
 - cert, 316
 - cert_url, 316
 - endElement, 315
 - req_resource_set_as, 316
 - req_resource_set_ipv4, 316
 - req_resource_set_ipv6, 316
 - startElement, 315
 - toXML, 316
- rpki::up_down::class_elt, 317
 - __init__, 318
 - cert_url, 319
 - certs, 319
 - class_name, 319
 - endElement, 318
 - from_resource_bag, 318
 - issuer, 319
 - resource_set_as, 319
 - resource_set_ipv4, 319
 - resource_set_ipv6, 319
 - resource_set_notafter, 320
 - startElement, 318
 - suggested_sia_head, 320
 - to_resource_bag, 318
 - toXML, 318
- rpki::up_down::class_response_syntax, 320
 - __init__, 321
 - classes, 321
 - startElement, 321
 - toXML, 321
- rpki::up_down::cms_msg, 321
 - encoding, 322
 - saxify, 322
 - schema, 322
- rpki::up_down::error_response_pdu, 322
 - __init__, 323
 - check_response, 323
 - codes, 324
 - description, 324
 - endElement, 323
 - exceptions, 324
 - status, 325
 - toXML, 324
- rpki::up_down::issue_pdu, 325
 - class_name, 327
 - endElement, 326
 - pkcs10, 327
 - query, 326
 - req_resource_set_as, 327
 - req_resource_set_ipv4, 327
 - req_resource_set_ipv6, 327
 - serve_pdu, 326
 - startElement, 326
 - toXML, 327
- rpki::up_down::issue_response_pdu, 328
 - check_response, 328
- rpki::up_down::list_pdu, 328
 - query, 329
 - serve_pdu, 329
 - toXML, 329
- rpki::up_down::list_response_pdu, 330
- rpki::up_down::message_pdu, 330
 - __str__, 331
 - make_query, 331
 - name2type, 332
 - payload, 332
 - recipient, 332
 - sender, 333
 - serve_error, 331
 - serve_top_level, 331

- startElement, 331
- toXML, 332
- type, 333
- type2name, 333
- version, 333
- rpki::up_down::multi_uri, 333
 - __init__, 334
 - __str__, 334
 - rsync, 334
- rpki::up_down::revoke_pdu, 335
 - class_name, 336
 - get_SKI, 335
 - query, 335
 - serve_pdu, 335
 - ski, 336
- rpki::up_down::revoke_response_pdu, 336
- rpki::up_down::revoke_syntax, 337
 - class_name, 338
 - ski, 338
 - startElement, 337
 - toXML, 337
- rpki::up_down::sax_handler, 338
 - name, 338
 - pdu, 339
 - version, 339
- rpki::x509
 - calculate_SKI, 94
 - POWify_OID, 94
- rpki::x509::CMS_object, 339
 - content, 342
 - debug_cms_certs, 342
 - DER, 342
 - dump_on_verify_failure, 342
 - econtent_oid, 343
 - extract, 340
 - formats, 343
 - get_content, 341
 - get_DER, 341
 - get_POW, 341
 - other_clear, 343
 - pem_converter, 343
 - POW, 344
 - print_on_der_error, 344
 - require_crls, 344
 - set_content, 341
 - sign, 341
 - verify, 342
- rpki::x509::CRL, 344
 - DER, 347
 - formats, 347
 - generate, 345
 - get_DER, 345
 - get_POW, 345
 - get_POWpkix, 346
 - getIssuer, 346
 - getNextUpdate, 346
 - getThisUpdate, 346
 - pem_converter, 347
 - POW, 347
 - POWpkix, 347
- rpki::x509::DER_CMS_object, 348
 - content, 349
 - decode, 348
 - encode, 348
- rpki::x509::DER_object, 349
 - __cmp__, 350
 - __init__, 350
 - clear, 350
 - DER, 355
 - dumpasn1, 351
 - empty, 351
 - formats, 355
 - from_sql, 351
 - gAKI, 351
 - get_3779resources, 351
 - get_AIA, 352
 - get_AKI, 352
 - get_Base64, 352
 - get_basicConstraints, 352
 - get_DER, 352
 - get_PEM, 353
 - get_SIA, 353
 - get_SKI, 353
 - gSKI, 353
 - hAKI, 354
 - hSKI, 354
 - is_CA, 354
 - other_clear, 355
 - pem_converter, 355
 - set, 354
 - to_sql, 355

- rpki::x509::PEM_converter, 356
 - __init__, 356
 - b, 357
 - e, 357
 - looks_like_PEM, 356
 - to_DER, 357
 - to_PEM, 357
- rpki::x509::PKCS10, 358
 - check_valid_rpki, 358
 - create, 359
 - create_ca, 359
 - DER, 360
 - formats, 360
 - get_DER, 359
 - get_POWpkix, 359
 - getPublicKey, 359
 - pem_converter, 360
 - POWpkix, 360
- rpki::x509::ROA, 361
 - build, 361
 - content_class, 361
 - econtent_oid, 361
 - pem_converter, 362
- rpki::x509::RSA, 362
 - DER, 364
 - formats, 364
 - generate, 363
 - get_DER, 363
 - get_POW, 363
 - get_public_DER, 363
 - get_RSAPublic, 364
 - get_SKI, 364
 - pem_converter, 364
 - POW, 365
- rpki::x509::RSAPublic, 365
 - DER, 367
 - formats, 367
 - get_DER, 366
 - get_POW, 366
 - get_SKI, 366
 - pem_converter, 367
 - POW, 367
- rpki::x509::SignedManifest, 367
 - build, 368
 - content_class, 369
 - econtent_oid, 369
 - getNextUpdate, 368
 - getThisUpdate, 368
 - pem_converter, 369
- rpki::x509::X509, 369
 - DER, 373
 - expired, 371
 - formats, 373
 - get_DER, 371
 - get_POW, 371
 - get_POWpkix, 371
 - getIssuer, 371
 - getNotAfter, 371
 - getNotBefore, 372
 - getPublicKey, 372
 - getSerial, 372
 - getSubject, 372
 - issue, 372
 - normalize_chain, 373
 - pem_converter, 373
 - POW, 374
 - POWpkix, 374
- rpki::x509::XML_CMS_object, 374
 - content, 376
 - decode, 375
 - dump_inbound_cms, 376
 - dump_outbound_cms, 377
 - dump_to_disk, 375
 - econtent_oid, 377
 - encode, 375
 - pretty_print_content, 375
 - schema_check, 376
 - unwrap, 376
 - wrap, 376
- rpki::xml_utils::base_elt, 377
 - __str__, 378
 - attributes, 380
 - booleans, 380
 - elements, 380
 - endElement, 378
 - make_b64elt, 378
 - make_elt, 379
 - make_pdu, 379
 - read_attrs, 379
 - startElement, 379
 - toXML, 379
- rpki::xml_utils::data_elt, 381

- endElement, 381
- make_reply, 382
- make_reply_clone_hook, 382
- serve_create, 382
- serve_destroy, 382
- serve_dispatch, 382
- serve_fetch_one, 383
- serve_get, 383
- serve_list, 383
- serve_post_save_hook, 383
- serve_pre_save_hook, 383
- serve_set, 384
- toXML, 384
- unimplemented_control, 384
- rpki::xml_utils::msg, 385
 - __str__, 385
 - endElement, 385
 - startElement, 385
 - toXML, 386
 - type, 386
 - version, 386
- rpki::xml_utils::sax_handler, 386
 - __init__, 387
 - characters, 387
 - create_top_level, 388
 - endElement, 388
 - endElementNS, 388
 - result, 389
 - saxify, 388
 - stack, 389
 - startElement, 388
 - startElementNS, 389
 - text, 389
- rpki_base_uri
 - rootd, 63
- rpki_class_name
 - rootd, 63
- rpki_content_type
 - rpki::https, 73
- rpki_engine.py(2502), 403
- rpki_root_cert
 - rootd, 63
- rpki_root_cert_uri
 - rootd, 64
- rpki_root_crl
 - rootd, 64
- rpki_root_dir
 - rootd, 64
- rpki_root_key
 - rootd, 64
- rpki_root_manifest
 - rootd, 64
- rpki_subject_cert
 - rootd, 64
- rpki_subject_lifetime
 - rootd, 65
- rpki_subject_pkcs10
 - rootd, 65
- rpki_subject_regen
 - rootd, 65
- rpkid, 95
 - cfg_file, 96
 - main, 96
 - profile, 96
- rpkid.py(2452), 403
- rpkid_cert
 - irbdb, 56
 - rpki::rpki_engine::rpkid_context, 293
- rpkid_key
 - rpki::rpki_engine::rpkid_context, 294
- rsync
 - rpki::up_down::multi_uri, 334
- runq
 - rpki::async::timer, 127
- saxify
 - irbe_cli::left_right_cms_msg, 106
 - irbe_cli::publication_cms_msg, 109
 - rootd::cms_msg, 118
 - rpki::left_right::cms_msg, 181
 - rpki::publication::cms_msg, 225
 - rpki::up_down::cms_msg, 322
 - rpki::xml_utils::sax_handler, 388
- schema
 - rpki::left_right::cms_msg, 181
 - rpki::publication::cms_msg, 225
 - rpki::up_down::cms_msg, 322
- schema_check
 - rpki::x509::XML_CMS_object, 376
- seconds_until_wakeup

- rpki::async::timer, 127
- select
 - rpki::sql::template, 305
- self
 - rpki::left_right::data_elt, 183
- self_handle
 - rpki::left_right::report_error_elt, 197
- self_id
 - rpki::left_right::data_elt, 184
- send
 - rpki::https::http_stream, 168
- send_error
 - rpki::https::http_server, 162
- send_message
 - rpki::https::http_server, 162
- send_reply
 - rpki::https::http_server, 162
- send_request
 - rpki::https::http_client, 148
 - rpki::https::http_queue, 156
- sender
 - rpki::up_down::message_pdu, 333
- Sequence, 390
- SequenceOf, 390
- serial
 - cross_certify, 48
 - rpki::rpki_engine::revoked_cert_obj, 289
- serial_file
 - cross_certify, 48
- serve_create
 - rpki::xml_utils::data_elt, 382
- serve_destroy
 - rpki::xml_utils::data_elt, 382
- serve_dispatch
 - rpki::publication::control_elt, 229
 - rpki::publication::publication_-object_elt, 234
 - rpki::xml_utils::data_elt, 382
- serve_error
 - rpki::up_down::message_pdu, 331
- serve_fetch_all
 - rpki::left_right::data_elt, 183
 - rpki::left_right::self_elt, 211
 - rpki::publication::client_elt, 222
- serve_fetch_handle
 - rpki::left_right::data_elt, 183
 - rpki::left_right::self_elt, 212
- serve_fetch_one
 - rpki::xml_utils::data_elt, 383
- serve_fetch_one_maybe
 - rpki::left_right::data_elt, 183
 - rpki::left_right::self_elt, 212
 - rpki::publication::client_elt, 222
 - rpki::publication::config_elt, 226
- serve_get
 - rpki::xml_utils::data_elt, 383
- serve_list
 - rpki::xml_utils::data_elt, 383
- serve_pdu
 - rootd::issue_pdu, 119
 - rootd::list_pdu, 120
 - rootd::revoke_pdu, 121
 - rpki::up_down::base_elt, 314
 - rpki::up_down::issue_pdu, 326
 - rpki::up_down::list_pdu, 329
 - rpki::up_down::revoke_pdu, 335
- serve_post_save_hook
 - rpki::left_right::child_elt, 178
 - rpki::left_right::parent_elt, 193
 - rpki::left_right::route_origin_elt, 204
 - rpki::left_right::self_elt, 212
 - rpki::publication::client_elt, 222
 - rpki::xml_utils::data_elt, 383
- serve_pre_save_hook
 - rpki::left_right::bsc_elt, 174
 - rpki::left_right::data_elt, 184
 - rpki::xml_utils::data_elt, 383
- serve_publish
 - rpki::publication::publication_-object_elt, 234
- serve_rekey
 - rpki::left_right::parent_elt, 193
 - rpki::left_right::self_elt, 212
- serve_revoke
 - rpki::left_right::parent_elt, 193
 - rpki::left_right::self_elt, 213
- serve_set
 - rpki::publication::config_elt, 226
 - rpki::xml_utils::data_elt, 384
- serve_top_level

- rpki::left_right::msg, 190
- rpki::publication::msg, 231
- rpki::up_down::message_pdu, 331
- serve_up_down
 - rpki::left_right::child_elt, 179
- serve_withdraw
 - rpki::publication::publication_object_elt, 234
- server
 - rpki::https, 72
- server_cert
 - irdbd, 56
 - rootd, 65
- server_ta
 - irbe_cli, 52
- set
 - rpki::async::timer, 127
 - rpki::x509::DER_object, 354
- set_content
 - rpki::x509::CMS_object, 341
- set_errback
 - rpki::async::timer, 127
- set_handler
 - rpki::async::timer, 128
- set_state
 - rpki::https::http_client, 148
- set_subject_cert
 - rootd, 61
- set_subject_pkcs10
 - rootd, 61
- set_trace
 - rpki::log, 77
- sia_uri
 - rpki::rpki_engine::ca_obj, 283
- sign
 - rpki::x509::CMS_object, 341
- signing_cert
 - irbe_cli::bsc_elt, 99
 - rpki::left_right::bsc_elt, 176
- signing_cert_crl
 - irbe_cli::bsc_elt, 99
 - rpki::left_right::bsc_elt, 176
- ski
 - rpki::up_down::revoke_pdu, 336
 - rpki::up_down::revoke_syntax, 338
- software_name
 - rpki::https::http_message, 154
- sql
 - pubd::pubd_context, 117
 - rpki::rpki_engine::rpkid_context, 294
 - sql.py(2502), 404
 - sql_debug
 - rpki::sql::sql_persistent, 303
 - sql_decode
 - rpki::rpki_engine::ca_detail_obj, 275
 - rpki::sql::sql_persistent, 299
 - sql_delete
 - rpki::sql::sql_persistent, 300
 - sql_delete_hook
 - rpki::left_right::route_origin_elt, 204
 - rpki::sql::sql_persistent, 300
 - sql_deleted
 - rpki::sql::sql_persistent, 303
 - sql_encode
 - rpki::sql::sql_persistent, 300
 - sql_fetch
 - rpki::sql::sql_persistent, 300
 - sql_fetch_all
 - rpki::sql::sql_persistent, 301
 - sql_fetch_hook
 - rpki::left_right::route_origin_elt, 204
 - rpki::sql::sql_persistent, 301
 - sql_fetch_where
 - rpki::sql::sql_persistent, 301
 - sql_fetch_where1
 - rpki::sql::sql_persistent, 301
 - sql_in_db
 - rpki::sql::sql_persistent, 304
 - sql_init
 - rpki::sql::sql_persistent, 301
 - sql_insert_hook
 - rpki::left_right::route_origin_elt, 204
 - rpki::sql::sql_persistent, 302
 - sql_is_dirty
 - rpki::sql::sql_persistent, 302
 - sql_mark_clean
 - rpki::sql::sql_persistent, 302

- sql_mark_deleted
 - rpki::sql::sql_persistent, 302
- sql_mark_dirty
 - rpki::sql::sql_persistent, 302
- sql_store
 - rpki::sql::sql_persistent, 303
- sql_template
 - rpki::left_right::bsc_elt, 176
 - rpki::left_right::child_elt, 180
 - rpki::left_right::parent_elt, 195
 - rpki::left_right::repository_elt, 200
 - rpki::left_right::route_origin_elt, 207
 - rpki::left_right::self_elt, 215
 - rpki::publication::client_elt, 224
 - rpki::publication::config_elt, 228
 - rpki::rpki_engine::ca_detail_obj, 277
 - rpki::rpki_engine::ca_obj, 283
 - rpki::rpki_engine::child_cert_obj, 286
 - rpki::rpki_engine::revoked_cert_obj, 289
- sql_update_hook
 - rpki::sql::sql_persistent, 303
- stack
 - rpki::xml_utils::sax_handler, 389
- start
 - rpki::https::http_client, 148
- startElement
 - rpki::left_right::list_resources_elt, 186
 - rpki::left_right::list_roa_requests_elt, 189
 - rpki::left_right::route_origin_elt, 205
 - rpki::publication::config_elt, 227
 - rpki::up_down::base_elt, 314
 - rpki::up_down::certificate_elt, 315
 - rpki::up_down::class_elt, 318
 - rpki::up_down::class_response_syntax, 321
 - rpki::up_down::issue_pdu, 326
 - rpki::up_down::message_pdu, 331
 - rpki::up_down::revoke_syntax, 337
 - rpki::xml_utils::base_elt, 379
 - rpki::xml_utils::msg, 385
 - rpki::xml_utils::sax_handler, 388
- startElementNS
 - rpki::xml_utils::sax_handler, 389
- startup_msg
 - irdbd, 56
- state
 - rpki::https::http_client, 150
 - rpki::rpki_engine::ca_detail_obj, 278
- status
 - rpki::up_down::error_response_pdu, 325
- suggested_sia_head
 - rpki::up_down::class_elt, 320
- sundial.py(2452), 404
- sweep
 - rpki::sql::session, 297
- symmetric_difference
 - rpki::resource_set::resource_set, 251
- ta
 - rpki::https::http_client, 150
 - rpki::https::http_listener, 152
 - rpki::https::http_queue, 157
- table
 - rpki::sql::template, 306
- tag
 - rpki::log, 78
- test
 - rpki::sundial, 90
- test1
 - rpki::resource_set, 86
- test2
 - rpki::resource_set, 86
- text
 - rpki::left_right::report_error_elt, 197
 - rpki::xml_utils::sax_handler, 389
- textwrap::TextWrapper, 390
- thisUpdate
 - rpki::manifest::Manifest, 219
- timeout
 - rpki::https::http_stream, 169
- timer
 - rpki::https::http_stream, 169
- tls

- rpki::https::http_client, 150
- rpki::https::http_server, 164
- rpki::https::http_stream, 169
- tls_accept
 - rpki::https::http_server, 163
- tls_connect
 - rpki::https::http_client, 148
- to_bytes
 - rpki::ipaddr::v4addr, 171
 - rpki::ipaddr::v6addr, 172
- to_DER
 - rpki::x509::PEM_converter, 357
- to_PEM
 - rpki::x509::PEM_converter, 357
- to_resource_bag
 - rpki::up_down::class_elt, 318
- to_resource_range
 - rpki::resource_set::roa_prefix, 259
- to_resource_set
 - rpki::resource_set::roa_prefix_set, 263
- to_rfc3779_tuple
 - rpki::resource_set::resource_range_as, 244
 - rpki::resource_set::resource_range_ip, 246
 - rpki::resource_set::resource_set_as, 253
 - rpki::resource_set::resource_set_ip, 255
- to_roa_tuple
 - rpki::resource_set::roa_prefix, 259
 - rpki::resource_set::roa_prefix_set, 263
- to_sql
 - rpki::sundial::datetime, 309
 - rpki::x509::DER_object, 355
- toASN1tuple
 - rpki::sundial::datetime, 309
- toGeneralizedTime
 - rpki::sundial::datetime, 309
- top_opts
 - irbe_cli, 52
- totimestamp
 - rpki::sundial::datetime, 309
- toUTCTime
 - rpki::sundial::datetime, 310
- toXML
 - rpki::left_right::list_resources_elt, 186
 - rpki::publication::publication_object_elt, 234
 - rpki::up_down::certificate_elt, 316
 - rpki::up_down::class_elt, 318
 - rpki::up_down::class_response_syntax, 321
 - rpki::up_down::error_response_pdu, 324
 - rpki::up_down::issue_pdu, 327
 - rpki::up_down::list_pdu, 329
 - rpki::up_down::message_pdu, 332
 - rpki::up_down::revoke_syntax, 337
 - rpki::xml_utils::base_elt, 379
 - rpki::xml_utils::data_elt, 384
 - rpki::xml_utils::msg, 386
- toXMLtime
 - rpki::sundial::datetime, 310
- trace
 - rpki::log, 77
- type
 - rpki::up_down::message_pdu, 333
 - rpki::xml_utils::msg, 386
- type2name
 - rootd::message_pdu, 121
 - rpki::up_down::message_pdu, 333
- u
 - irdbd, 56
- undersized
 - rpki::resource_set::resource_bag, 241
- unimplemented_control
 - rpki::left_right::data_elt, 184
 - rpki::xml_utils::data_elt, 384
- union
 - rpki::resource_set::resource_bag, 241
 - rpki::resource_set::resource_set, 251
- unwrap
 - rpki::x509::XML_CMS_object, 376
- up_down
 - rpki::relaxng, 83

- up_down.py(2499), [405](#)
- up_down_handler
 - rootd, [61](#)
 - rpki::rpki_engine::rpkid_context, [292](#)
- up_down_url_regexp
 - rpki::rpki_engine::rpkid_context, [294](#)
- update
 - rpki::rpki_engine::ca_detail_obj, [275](#)
 - rpki::sql::template, [306](#)
- update_children
 - rpki::left_right::self_elt, [213](#)
- update_roa
 - rpki::left_right::route_origin_elt, [205](#)
- update_roas
 - rpki::left_right::self_elt, [213](#)
- update_timeout
 - rpki::https::http_stream, [168](#)
- uri
 - rpki::rpki_engine::child_cert_obj, [285](#)
- uri_tail
 - rpki::rpki_engine::child_cert_obj, [286](#)
- uri_to_filename
 - rpki::publication::publication_object_elt, [235](#)
- url
 - irbe_cli, [52](#)
- usage
 - cross_certify, [46](#)
 - irbe_cli, [50](#)
 - irbe_cli::cmd_elt_mixin, [102](#)
 - irbe_cli::cmd_msg_mixin, [104](#)
- usage_fill
 - irbe_cli, [52](#)
- use_hsm
 - rpki::left_right::self_elt, [215](#)
- use_syslog
 - rpki::log, [79](#)
- username
 - rpki::sql::session, [298](#)
- v4
 - rpki::resource_set::resource_bag, [241](#)
- v6
 - rpki::resource_set::resource_bag, [242](#)
- valid_until
 - rpki::left_right::list_resources_elt, [188](#)
 - rpki::resource_set::resource_bag, [242](#)
- value
 - cross_certify, [48](#)
- verbose
 - irbe_cli, [53](#)
- verify
 - rpki::x509::CMS_object, [342](#)
- version
 - rpki::https::http_message, [155](#)
 - rpki::left_right::msg, [191](#)
 - rpki::left_right::sax_handler, [208](#)
 - rpki::manifest::Manifest, [219](#)
 - rpki::publication::msg, [232](#)
 - rpki::publication::sax_handler, [238](#)
 - rpki::roa::RouteOriginAttestation, [270](#)
 - rpki::up_down::message_pdu, [333](#)
 - rpki::up_down::sax_handler, [339](#)
 - rpki::xml_utils::msg, [386](#)
- want_persistent_client
 - rpki::https, [73](#)
- want_persistent_server
 - rpki::https, [73](#)
- warn
 - rpki::log, [79](#)
- when
 - rpki::async::timer, [128](#)
- wired_in_config_id
 - rpki::publication::config_elt, [228](#)
- withdraw
 - rpki::left_right::repository_elt, [199](#)
- withdraw_roa
 - rpki::left_right::route_origin_elt, [205](#)
- wrap

- rpki::x509::XML_CMS_object, [376](#)
- writeable
 - rpki::https::http_stream, [168](#)
- x
 - cross_certify, [48](#)
- x509.py(2496), [405](#)
- xml::sax::handler::ContentHandler, [390](#)
- xml_utils.py(2493), [406](#)
- xmlns
 - rpki::left_right::left_right_
namespace, [185](#)
 - rpki::publication::publication_
namespace, [233](#)
 - rpki::up_down, [92](#)