

# RPKI Engine

## 1.0

Generated by Doxygen 1.5.8

Thu Jun 4 06:15:50 2009

## Contents

<b>1</b>	<b>RPKI Engine Reference Manual</b>	<b>1</b>
<b>2</b>	<b>Further Reading</b>	<b>1</b>
<b>3</b>	<b>Installation Guide</b>	<b>2</b>
<b>4</b>	<b>Operation Guide</b>	<b>4</b>
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
<b>5</b>	<b>Left-right protocol</b>	<b>18</b>
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
<b>6</b>	<b>Publication protocol</b>	<b>28</b>

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
<b>7</b>	<b>SQL database schemas</b>	<b>32</b>
7.1	rpkid SQL schema . . . . .	34
7.2	pubd SQL Schema . . . . .	38
7.3	irdbd SQL Schema . . . . .	40
<b>8</b>	<b>BPKI model</b>	<b>41</b>
<b>9</b>	<b>Namespace Documentation</b>	<b>44</b>
9.1	Package cross_certify . . . . .	44
9.1.1	Detailed Description . . . . .	45
9.1.2	Function Documentation . . . . .	45
9.1.3	Variable Documentation . . . . .	46
9.2	Package irbe_cli . . . . .	48
9.2.1	Detailed Description . . . . .	49
9.2.2	Function Documentation . . . . .	50
9.2.3	Variable Documentation . . . . .	50
9.3	Package irdbd . . . . .	52
9.3.1	Detailed Description . . . . .	53
9.3.2	Function Documentation . . . . .	54
9.3.3	Variable Documentation . . . . .	54

9.4	Package pubd	56
9.4.1	Detailed Description	56
9.4.2	Function Documentation	57
9.4.3	Variable Documentation	57
9.5	Package rootd	58
9.5.1	Detailed Description	59
9.5.2	Function Documentation	60
9.5.3	Variable Documentation	61
9.6	Package rpki	65
9.7	Package rpki.async	65
9.7.1	Detailed Description	66
9.7.2	Function Documentation	66
9.7.3	Variable Documentation	67
9.8	Package rpki.config	67
9.8.1	Detailed Description	67
9.9	Package rpki.exceptions	68
9.9.1	Detailed Description	69
9.10	Package rpki.https	69
9.10.1	Detailed Description	70
9.10.2	Function Documentation	71
9.10.3	Variable Documentation	72
9.11	Package rpki.ipaddrs	73
9.11.1	Detailed Description	73
9.12	Package rpki.left_right	74
9.12.1	Detailed Description	74
9.12.2	Variable Documentation	75
9.13	Package rpki.log	75
9.13.1	Detailed Description	76
9.13.2	Function Documentation	76
9.13.3	Variable Documentation	77
9.14	Package rpki.manifest	78

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

9.26.1 Detailed Description . . . . .	94
9.26.2 Function Documentation . . . . .	95
9.26.3 Variable Documentation . . . . .	95
<b>10 Class Documentation</b>	<b>96</b>
10.1 asynchat.async_chat Class Reference . . . . .	96
10.2 asyncore.dispatcher Class Reference . . . . .	96
10.3 ConfigParser.RawConfigParser Class Reference . . . . .	96
10.4 Exception Class Reference . . . . .	96
10.5 irbe_cli.bsc_elt Class Reference . . . . .	96
10.5.1 Detailed Description . . . . .	97
10.5.2 Member Function Documentation . . . . .	97
10.5.3 Member Data Documentation . . . . .	98
10.6 irbe_cli.certificate_elt Class Reference . . . . .	98
10.6.1 Detailed Description . . . . .	99
10.7 irbe_cli.child_elt Class Reference . . . . .	99
10.7.1 Detailed Description . . . . .	99
10.8 irbe_cli.client_elt Class Reference . . . . .	99
10.8.1 Detailed Description . . . . .	99
10.9 irbe_cli.cmd_elt_mixin Class Reference . . . . .	99
10.9.1 Detailed Description . . . . .	100
10.9.2 Member Function Documentation . . . . .	100
10.9.3 Member Data Documentation . . . . .	102
10.10 irbe_cli.cmd_msg_mixin Class Reference . . . . .	103
10.10.1 Detailed Description . . . . .	104
10.10.2 Member Function Documentation . . . . .	104
10.11 irbe_cli.config_elt Class Reference . . . . .	104
10.11.1 Detailed Description . . . . .	104
10.11.2 Member Function Documentation . . . . .	105
10.11.3 Member Data Documentation . . . . .	105
10.12 irbe_cli.crl_elt Class Reference . . . . .	105

10.12.1 Detailed Description . . . . .	105
10.13irbe_cli.left_right_cms_msg Class Reference . . . . .	105
10.13.1 Detailed Description . . . . .	106
10.13.2 Member Data Documentation . . . . .	106
10.14irbe_cli.left_right_msg Class Reference . . . . .	106
10.14.1 Detailed Description . . . . .	106
10.14.2 Member Data Documentation . . . . .	106
10.15irbe_cli.left_right_sax_handler Class Reference . . . . .	107
10.15.1 Detailed Description . . . . .	107
10.15.2 Member Data Documentation . . . . .	107
10.16irbe_cli.manifest_elt Class Reference . . . . .	107
10.16.1 Detailed Description . . . . .	107
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 . . . . .	108
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 . . . . .	109
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 . . . . .	110
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	<a href="#">irbe_cli.self_elt Class Reference</a>	112
10.24.1	<a href="#">Detailed Description</a>	112
10.25	<a href="#">irbe_cli.UsageWrapper Class Reference</a>	113
10.25.1	<a href="#">Detailed Description</a>	113
10.25.2	<a href="#">Member Function Documentation</a>	113
10.26	<a href="#">long Class Reference</a>	113
10.27	<a href="#">object Class Reference</a>	113
10.28	<a href="#">pubd.pubd_context Class Reference</a>	114
10.28.1	<a href="#">Detailed Description</a>	115
10.28.2	<a href="#">Member Function Documentation</a>	115
10.28.3	<a href="#">Member Data Documentation</a>	116
10.29	<a href="#">pydatetime.datetime Class Reference</a>	117
10.30	<a href="#">pydatetime.timedelta Class Reference</a>	117
10.31	<a href="#">rootd.cms_msg Class Reference</a>	118
10.31.1	<a href="#">Detailed Description</a>	118
10.31.2	<a href="#">Member Data Documentation</a>	118
10.32	<a href="#">rootd.issue_pdu Class Reference</a>	118
10.32.1	<a href="#">Detailed Description</a>	118
10.32.2	<a href="#">Member Function Documentation</a>	119
10.33	<a href="#">rootd.list_pdu Class Reference</a>	119
10.33.1	<a href="#">Detailed Description</a>	119
10.33.2	<a href="#">Member Function Documentation</a>	119
10.34	<a href="#">rootd.message_pdu Class Reference</a>	120
10.34.1	<a href="#">Detailed Description</a>	120
10.34.2	<a href="#">Member Data Documentation</a>	120
10.35	<a href="#">rootd.revoke_pdu Class Reference</a>	121
10.35.1	<a href="#">Detailed Description</a>	121
10.35.2	<a href="#">Member Function Documentation</a>	121
10.36	<a href="#">rootd.sax_handler Class Reference</a>	121
10.36.1	<a href="#">Detailed Description</a>	121
10.36.2	<a href="#">Member Data Documentation</a>	122



10.37rpki.async.iterator Class Reference . . . . .	122
10.37.1 Detailed Description . . . . .	122
10.37.2 Member Function Documentation . . . . .	123
10.37.3 Member Data Documentation . . . . .	123
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 . . . . .	128
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 . . . . .	130
10.41.1 Detailed Description . . . . .	130
10.42rpki.exceptions.BadContactURL Class Reference . . . . .	130
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 . . . . .	131
10.44.1 Detailed Description . . . . .	131
10.45rpki.exceptions.BadIssueResponse Class Reference . . . . .	131
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 . . . . .	132
10.47.1 Detailed Description . . . . .	132
10.48rpki.exceptions.BadQuery Class Reference . . . . .	132
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 . . . . .	133
10.50.1 Detailed Description . . . . .	133
10.51rpki.exceptions.BadURISyntax Class Reference . . . . .	133
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 . . . . .	134
10.53.1 Detailed Description . . . . .	134
10.54rpki.exceptions.ClassNameMismatch Class Reference . . . . .	134
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 . . . . .	135
10.56.1 Detailed Description . . . . .	135
10.57rpki.exceptions.CMSCRLNotSet Class Reference . . . . .	135
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 . . . . .	136
10.59.1 Detailed Description . . . . .	136
10.60rpki.exceptions.DERObjectConversionError Class Reference . . . . .	136
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 . . . . .	137
10.62.1 Detailed Description . . . . .	137
10.63rpki.exceptions.ForbiddenURI Class Reference . . . . .	137
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 . . . . .	138
10.65.1 Detailed Description . . . . .	138
10.66rpki.exceptions.MissingCMSCRL Class Reference . . . . .	138
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 . . . . .	139
10.68.1 Detailed Description . . . . .	139
10.69rpki.exceptions.MustBePrefix Class Reference . . . . .	139
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 . . . . .	140
10.71.1 Detailed Description . . . . .	140
10.72rpki.exceptions.NotFound Class Reference . . . . .	140
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 . . . . .	141
10.74.1 Detailed Description . . . . .	141
10.75rpki.exceptions.ReceivedTLSCACert Class Reference . . . . .	141
10.75.1 Detailed Description . . . . .	142
10.76rpki.exceptions.RPKI_Exception Class Reference . . . . .	142
10.76.1 Detailed Description . . . . .	142
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 . . . . .	143
10.79.1 Detailed Description . . . . .	143
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 . . . . .	144
10.82rpki.exceptions.UnexpectedCMSCRLs Class Reference . . . . .	144
10.82.1 Detailed Description . . . . .	144
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 . . . . .	145
10.85rpki.exceptions.WrongEContentType Class Reference . . . . .	145
10.85.1 Detailed Description . . . . .	145
10.86rpki.https.http_client Class Reference . . . . .	146
10.86.1 Detailed Description . . . . .	146
10.86.2 Member Function Documentation . . . . .	147
10.86.3 Member Data Documentation . . . . .	148
10.87rpki.https.http_listener Class Reference . . . . .	150
10.87.1 Detailed Description . . . . .	150
10.87.2 Member Function Documentation . . . . .	151
10.87.3 Member Data Documentation . . . . .	151
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 . . . . .	154
10.89.1 Detailed Description . . . . .	155
10.89.2 Member Function Documentation . . . . .	155
10.89.3 Member Data Documentation . . . . .	156
10.90rpki.https.http_request Class Reference . . . . .	157
10.90.1 Detailed Description . . . . .	157
10.90.2 Member Function Documentation . . . . .	158
10.90.3 Member Data Documentation . . . . .	158

10.91rpki.https.http_response Class Reference . . . . .	159
10.91.1 Detailed Description . . . . .	159
10.91.2 Member Function Documentation . . . . .	159
10.91.3 Member Data Documentation . . . . .	160
10.92rpki.https.http_server Class Reference . . . . .	160
10.92.1 Detailed Description . . . . .	161
10.92.2 Member Function Documentation . . . . .	161
10.92.3 Member Data Documentation . . . . .	162
10.93rpki.https.http_stream Class Reference . . . . .	163
10.93.1 Detailed Description . . . . .	164
10.93.2 Member Function Documentation . . . . .	164
10.93.3 Member Data Documentation . . . . .	168
10.94rpki.ipaddrs.v4addr Class Reference . . . . .	169
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 . . . . .	171
10.95.2 Member Function Documentation . . . . .	171
10.95.3 Member Data Documentation . . . . .	172
10.96rpki.left_right.bsc_elt Class Reference . . . . .	172
10.96.1 Detailed Description . . . . .	173
10.96.2 Member Function Documentation . . . . .	173
10.96.3 Member Data Documentation . . . . .	174
10.97rpki.left_right.child_elt Class Reference . . . . .	176
10.97.1 Detailed Description . . . . .	177
10.97.2 Member Function Documentation . . . . .	177
10.97.3 Member Data Documentation . . . . .	178
10.98rpki.left_right.cms_msg Class Reference . . . . .	180
10.98.1 Detailed Description . . . . .	180
10.98.2 Member Data Documentation . . . . .	180

10.99	rpki.left_right.data_elt Class Reference . . . . .	181
10.99.1	Detailed Description . . . . .	182
10.99.2	Member Function Documentation . . . . .	182
10.99.3	Member Data Documentation . . . . .	183
10.100	rpki.left_right.left_right_namespace Class Reference . . . . .	184
10.100.1	Detailed Description . . . . .	184
10.100.2	Member Data Documentation . . . . .	184
10.101	rpki.left_right.list_resources_elt Class Reference . . . . .	184
10.101.1	Detailed Description . . . . .	185
10.101.2	Member Function Documentation . . . . .	185
10.101.3	Member Data Documentation . . . . .	186
10.102	rpki.left_right.msg Class Reference . . . . .	187
10.102.1	Detailed Description . . . . .	187
10.102.2	Member Function Documentation . . . . .	188
10.102.3	Member Data Documentation . . . . .	188
10.103	rpki.left_right.parent_elt Class Reference . . . . .	188
10.103.1	Detailed Description . . . . .	189
10.103.2	Member Function Documentation . . . . .	189
10.103.3	Member Data Documentation . . . . .	191
10.104	rpki.left_right.report_error_elt Class Reference . . . . .	192
10.104.1	Detailed Description . . . . .	193
10.104.2	Member Function Documentation . . . . .	193
10.104.3	Member Data Documentation . . . . .	193
10.105	rpki.left_right.repository_elt Class Reference . . . . .	194
10.105.1	Detailed Description . . . . .	195
10.105.2	Member Function Documentation . . . . .	195
10.105.3	Member Data Documentation . . . . .	196
10.106	rpki.left_right.route_origin_elt Class Reference . . . . .	198
10.106.1	Detailed Description . . . . .	199
10.106.2	Member Function Documentation . . . . .	199
10.106.3	Member Data Documentation . . . . .	202

10.107	<a href="#">rpkil.left_right.sax_handler Class Reference</a>	204
10.107.1	<a href="#">Detailed Description</a>	205
10.107.2	<a href="#">Member Data Documentation</a>	205
10.108	<a href="#">rpkil.left_right.self_elt Class Reference</a>	205
10.108.1	<a href="#">Detailed Description</a>	207
10.108.2	<a href="#">Member Function Documentation</a>	207
10.108.3	<a href="#">Member Data Documentation</a>	210
10.109	<a href="#">rpkil.log.logger Class Reference</a>	212
10.109.1	<a href="#">Detailed Description</a>	213
10.109.2	<a href="#">Member Function Documentation</a>	213
10.109.3	<a href="#">Member Data Documentation</a>	213
10.110	<a href="#">rpkil.manifest.FileAndHash Class Reference</a>	213
10.110.1	<a href="#">Detailed Description</a>	214
10.110.2	<a href="#">Member Function Documentation</a>	214
10.110.3	<a href="#">Member Data Documentation</a>	214
10.111	<a href="#">rpkil.manifest.FilesAndHashes Class Reference</a>	214
10.111.1	<a href="#">Detailed Description</a>	215
10.111.2	<a href="#">Member Function Documentation</a>	215
10.112	<a href="#">rpkil.manifest.Manifest Class Reference</a>	215
10.112.1	<a href="#">Detailed Description</a>	215
10.112.2	<a href="#">Member Function Documentation</a>	216
10.112.3	<a href="#">Member Data Documentation</a>	216
10.113	<a href="#">rpkil.publication.certificate_elt Class Reference</a>	217
10.113.1	<a href="#">Detailed Description</a>	217
10.113.2	<a href="#">Member Data Documentation</a>	217
10.114	<a href="#">rpkil.publication.client_elt Class Reference</a>	218
10.114.1	<a href="#">Detailed Description</a>	218
10.114.2	<a href="#">Member Function Documentation</a>	218
10.114.3	<a href="#">Member Data Documentation</a>	220
10.115	<a href="#">rpkil.publication.cms_msg Class Reference</a>	221
10.115.1	<a href="#">Detailed Description</a>	221

10.115.	Member Data Documentation	222
10.116.	pkpublication.config_elt Class Reference	222
10.116.	Detailed Description	223
10.116.	Member Function Documentation	223
10.116.	Member Data Documentation	224
10.117.	pkpublication.control_elt Class Reference	225
10.117.	Detailed Description	225
10.117.	Member Function Documentation	226
10.118.	pkpublication.crl_elt Class Reference	226
10.118.	Detailed Description	226
10.118.	Member Data Documentation	226
10.119.	pkpublication.manifest_elt Class Reference	227
10.119.	Detailed Description	227
10.119.	Member Data Documentation	227
10.120.	pkpublication.msg Class Reference	228
10.120.	Detailed Description	228
10.120.	Member Function Documentation	228
10.120.	Member Data Documentation	228
10.121.	pkpublication.publication_namespace Class Reference	229
10.121.	Detailed Description	229
10.121.	Member Data Documentation	229
10.122.	pkpublication.publication_object_elt Class Reference	230
10.122.	Detailed Description	230
10.122.	Member Function Documentation	231
10.122.	Member Data Documentation	232
10.123.	pkpublication.report_error_elt Class Reference	232
10.123.	Detailed Description	233
10.123.	Member Function Documentation	233
10.123.	Member Data Documentation	233
10.124.	pkpublication.roa_elt Class Reference	234
10.124.	Detailed Description	234



10.124.	Member Data Documentation	234
10.125.	rpki.publication.sax_handler Class Reference	235
10.125.	Detailed Description	235
10.125.	Member Data Documentation	235
10.126.	rpki.resource_set.resource_bag Class Reference	236
10.126.	Detailed Description	236
10.126.	Member Function Documentation	237
10.126.	Member Data Documentation	238
10.127.	rpki.resource_set.resource_range Class Reference	239
10.127.	Detailed Description	240
10.127.	Member Function Documentation	240
10.127.	Member Data Documentation	240
10.128.	rpki.resource_set.resource_range_as Class Reference	241
10.128.	Detailed Description	241
10.128.	Member Function Documentation	241
10.128.	Member Data Documentation	242
10.129.	rpki.resource_set.resource_range_ip Class Reference	242
10.129.	Detailed Description	243
10.129.	Member Function Documentation	243
10.130.	rpki.resource_set.resource_range_ipv4 Class Reference	244
10.130.	Detailed Description	244
10.130.	Member Data Documentation	244
10.131.	rpki.resource_set.resource_range_ipv6 Class Reference	245
10.131.	Detailed Description	245
10.131.	Member Data Documentation	245
10.132.	rpki.resource_set.resource_set Class Reference	245
10.132.	Detailed Description	246
10.132.	Member Function Documentation	246
10.132.	Member Data Documentation	249
10.133.	rpki.resource_set.resource_set_as Class Reference	249
10.133.	Detailed Description	249

10.133.2	Member Function Documentation . . . . .	250
10.133.3	Member Data Documentation . . . . .	250
10.134	rpki.resource_set.resource_set_ip Class Reference . . . . .	251
10.134.1	Detailed Description . . . . .	251
10.134.2	Member Function Documentation . . . . .	251
10.134.3	Member Data Documentation . . . . .	252
10.135	rpki.resource_set.resource_set_ipv4 Class Reference . . . . .	252
10.135.1	Detailed Description . . . . .	253
10.135.2	Member Data Documentation . . . . .	253
10.136	rpki.resource_set.resource_set_ipv6 Class Reference . . . . .	253
10.136.1	Detailed Description . . . . .	254
10.136.2	Member Data Documentation . . . . .	254
10.137	rpki.resource_set.roa_prefix Class Reference . . . . .	254
10.137.1	Detailed Description . . . . .	255
10.137.2	Member Function Documentation . . . . .	255
10.137.3	Member Data Documentation . . . . .	257
10.138	rpki.resource_set.roa_prefix_ipv4 Class Reference . . . . .	257
10.138.1	Detailed Description . . . . .	257
10.138.2	Member Data Documentation . . . . .	258
10.139	rpki.resource_set.roa_prefix_ipv6 Class Reference . . . . .	258
10.139.1	Detailed Description . . . . .	258
10.139.2	Member Data Documentation . . . . .	258
10.140	rpki.resource_set.roa_prefix_set Class Reference . . . . .	259
10.140.1	Detailed Description . . . . .	259
10.140.2	Member Function Documentation . . . . .	259
10.141	rpki.resource_set.roa_prefix_set_ipv4 Class Reference . . . . .	261
10.141.1	Detailed Description . . . . .	261
10.141.2	Member Data Documentation . . . . .	261
10.142	rpki.resource_set.roa_prefix_set_ipv6 Class Reference . . . . .	262
10.142.1	Detailed Description . . . . .	262
10.142.2	Member Data Documentation . . . . .	262

10.143	rpki.roa.ROAIPAddress Class Reference . . . . .	263
10.143.1	Detailed Description . . . . .	263
10.143.2	Member Function Documentation . . . . .	263
10.143.3	Member Data Documentation . . . . .	263
10.144	rpki.roa.ROAIPAddresses Class Reference . . . . .	264
10.144.1	Detailed Description . . . . .	264
10.144.2	Member Function Documentation . . . . .	264
10.145	rpki.roa.ROAIPAddressFamilies Class Reference . . . . .	264
10.145.1	Detailed Description . . . . .	264
10.145.2	Member Function Documentation . . . . .	265
10.146	rpki.roa.ROAIPAddressFamily Class Reference . . . . .	265
10.146.1	Detailed Description . . . . .	265
10.146.2	Member Function Documentation . . . . .	265
10.146.3	Member Data Documentation . . . . .	266
10.147	rpki.roa.RouteOriginAttestation Class Reference . . . . .	266
10.147.1	Detailed Description . . . . .	266
10.147.2	Member Function Documentation . . . . .	266
10.147.3	Member Data Documentation . . . . .	267
10.148	rpki.rpki_engine.ca_detail_obj Class Reference . . . . .	267
10.148.1	Detailed Description . . . . .	268
10.148.2	Member Function Documentation . . . . .	269
10.148.3	Member Data Documentation . . . . .	273
10.149	rpki.rpki_engine.ca_obj Class Reference . . . . .	275
10.149.1	Detailed Description . . . . .	276
10.149.2	Member Function Documentation . . . . .	276
10.149.3	Member Data Documentation . . . . .	279
10.150	rpki.rpki_engine.child_cert_obj Class Reference . . . . .	280
10.150.1	Detailed Description . . . . .	281
10.150.2	Member Function Documentation . . . . .	281
10.150.3	Member Data Documentation . . . . .	283
10.151	rpki.rpki_engine.revoked_cert_obj Class Reference . . . . .	284

10.151.	Detailed Description . . . . .	285
10.151.	Member Function Documentation . . . . .	285
10.151.	Member Data Documentation . . . . .	285
10.152.	rpki.rpki_engine.rpkid_context Class Reference . . . . .	287
10.152.	Detailed Description . . . . .	287
10.152.	Member Function Documentation . . . . .	288
10.152.	Member Data Documentation . . . . .	289
10.153.	rpki.sql.session Class Reference . . . . .	291
10.153.	Detailed Description . . . . .	292
10.153.	Member Function Documentation . . . . .	292
10.153.	Member Data Documentation . . . . .	294
10.154.	rpki.sql.sql_persistent Class Reference . . . . .	295
10.154.	Detailed Description . . . . .	296
10.154.	Member Function Documentation . . . . .	296
10.154.	Member Data Documentation . . . . .	300
10.155.	rpki.sql.template Class Reference . . . . .	301
10.155.	Detailed Description . . . . .	301
10.155.	Member Function Documentation . . . . .	301
10.155.	Member Data Documentation . . . . .	301
10.156.	rpki.sundial.datetime Class Reference . . . . .	303
10.156.	Detailed Description . . . . .	303
10.156.	Member Function Documentation . . . . .	303
10.156.	Member Data Documentation . . . . .	307
10.157.	rpki.sundial.timedelta Class Reference . . . . .	307
10.157.	Detailed Description . . . . .	307
10.157.	Member Function Documentation . . . . .	308
10.157.	Member Data Documentation . . . . .	308
10.158.	rpki.up_down.base_elt Class Reference . . . . .	309
10.158.	Detailed Description . . . . .	309
10.158.	Member Function Documentation . . . . .	310
10.159.	rpki.up_down.certificate_elt Class Reference . . . . .	311

10.159.Detailed Description . . . . .	312
10.159.2Member Function Documentation . . . . .	312
10.159.3Member Data Documentation . . . . .	313
10.160pk_i.up_down.class_elt Class Reference . . . . .	313
10.160.Detailed Description . . . . .	314
10.160.2Member Function Documentation . . . . .	314
10.160.3Member Data Documentation . . . . .	315
10.161pk_i.up_down.class_response_syntax Class Reference . . . . .	317
10.161.Detailed Description . . . . .	317
10.161.2Member Function Documentation . . . . .	317
10.161.3Member Data Documentation . . . . .	318
10.162pk_i.up_down.cms_msg Class Reference . . . . .	318
10.162.Detailed Description . . . . .	319
10.162.2Member Data Documentation . . . . .	319
10.163pk_i.up_down.error_response_pdu Class Reference . . . . .	319
10.163.Detailed Description . . . . .	320
10.163.2Member Function Documentation . . . . .	320
10.163.3Member Data Documentation . . . . .	321
10.164pk_i.up_down.issue_pdu Class Reference . . . . .	322
10.164.Detailed Description . . . . .	322
10.164.2Member Function Documentation . . . . .	323
10.164.3Member Data Documentation . . . . .	324
10.165pk_i.up_down.issue_response_pdu Class Reference . . . . .	325
10.165.Detailed Description . . . . .	325
10.165.2Member Function Documentation . . . . .	325
10.166pk_i.up_down.list_pdu Class Reference . . . . .	325
10.166.Detailed Description . . . . .	326
10.166.2Member Function Documentation . . . . .	326
10.167pk_i.up_down.list_response_pdu Class Reference . . . . .	326
10.167.Detailed Description . . . . .	327
10.168pk_i.up_down.message_pdu Class Reference . . . . .	327

10.168.Detailed Description . . . . .	327
10.168.2Member Function Documentation . . . . .	328
10.168.3Member Data Documentation . . . . .	329
10.169Rpki.up_down.multi_uri Class Reference . . . . .	330
10.169.Detailed Description . . . . .	331
10.169.2Member Function Documentation . . . . .	331
10.170Rpki.up_down.revoke_pdu Class Reference . . . . .	332
10.170.Detailed Description . . . . .	332
10.170.2Member Function Documentation . . . . .	332
10.170.3Member Data Documentation . . . . .	333
10.171Rpki.up_down.revoke_response_pdu Class Reference . . . . .	333
10.171.Detailed Description . . . . .	333
10.172Rpki.up_down.revoke_syntax Class Reference . . . . .	334
10.172.Detailed Description . . . . .	334
10.172.2Member Function Documentation . . . . .	334
10.172.3Member Data Documentation . . . . .	335
10.173Rpki.up_down.sax_handler Class Reference . . . . .	335
10.173.Detailed Description . . . . .	335
10.173.2Member Data Documentation . . . . .	335
10.174Rpki.x509.CMS_object Class Reference . . . . .	336
10.174.Detailed Description . . . . .	337
10.174.2Member Function Documentation . . . . .	337
10.174.3Member Data Documentation . . . . .	339
10.175Rpki.x509.CRL Class Reference . . . . .	341
10.175.Detailed Description . . . . .	342
10.175.2Member Function Documentation . . . . .	342
10.175.3Member Data Documentation . . . . .	344
10.176Rpki.x509.DER_CMS_object Class Reference . . . . .	345
10.176.Detailed Description . . . . .	345
10.176.2Member Function Documentation . . . . .	345
10.176.3Member Data Documentation . . . . .	346

10.177	pkix509.DER_object Class Reference . . . . .	346
10.177.1	Detailed Description . . . . .	347
10.177.2	Member Function Documentation . . . . .	347
10.177.3	Member Data Documentation . . . . .	352
10.178	pkix509.PEM_converter Class Reference . . . . .	353
10.178.1	Detailed Description . . . . .	353
10.178.2	Member Function Documentation . . . . .	353
10.178.3	Member Data Documentation . . . . .	354
10.179	pkix509.PKCS10 Class Reference . . . . .	355
10.179.1	Detailed Description . . . . .	355
10.179.2	Member Function Documentation . . . . .	355
10.179.3	Member Data Documentation . . . . .	357
10.180	pkix509.ROA Class Reference . . . . .	358
10.180.1	Detailed Description . . . . .	358
10.180.2	Member Function Documentation . . . . .	358
10.180.3	Member Data Documentation . . . . .	358
10.181	pkix509.RSA Class Reference . . . . .	359
10.181.1	Detailed Description . . . . .	360
10.181.2	Member Function Documentation . . . . .	360
10.181.3	Member Data Documentation . . . . .	361
10.182	pkix509.RSAPublic 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.SignedManifest Class Reference . . . . .	365
10.183.1	Detailed Description . . . . .	365
10.183.2	Member Function Documentation . . . . .	365
10.183.3	Member Data Documentation . . . . .	366
10.184	pkix509.X509 Class Reference . . . . .	367
10.184.1	Detailed Description . . . . .	368
10.184.2	Member Function Documentation . . . . .	368

10.184.3Member Data Documentation . . . . .	370
10.185pkix509.XML_CMS_object Class Reference . . . . .	372
10.185.1Detailed Description . . . . .	372
10.185.2Member Function Documentation . . . . .	372
10.185.3Member Data Documentation . . . . .	374
10.186pkixml_utils.base_elt Class Reference . . . . .	375
10.186.1Detailed Description . . . . .	375
10.186.2Member Function Documentation . . . . .	376
10.186.3Member Data Documentation . . . . .	377
10.187pkixml_utils.data_elt Class Reference . . . . .	378
10.187.1Detailed Description . . . . .	379
10.187.2Member Function Documentation . . . . .	379
10.188pkixml_utils.msg Class Reference . . . . .	382
10.188.1Detailed Description . . . . .	383
10.188.2Member Function Documentation . . . . .	383
10.188.3Member Data Documentation . . . . .	384
10.189pkixml_utils.sax_handler Class Reference . . . . .	384
10.189.1Detailed Description . . . . .	385
10.189.2Member Function Documentation . . . . .	385
10.189.3Member Data Documentation . . . . .	387
10.190Sequence Class Reference . . . . .	387
10.191SequenceOf Class Reference . . . . .	388
10.192textwrap.TextWrapper Class Reference . . . . .	388
10.193xml.sax.handler.ContentHandler Class Reference . . . . .	388
<b>11 File Documentation</b>	<b>388</b>
11.1 __init__.py File Reference . . . . .	388
11.2 async.py File Reference . . . . .	388
11.3 config.py File Reference . . . . .	389
11.4 cross_certify.py File Reference . . . . .	389
11.5 exceptions.py File Reference . . . . .	390



11.6 https.py File Reference . . . . .	391
11.7 ipaddrs.py File Reference . . . . .	392
11.8 irbe_cli.py File Reference . . . . .	392
11.9 irdbd.py File Reference . . . . .	393
11.10left_right.py File Reference . . . . .	394
11.11log.py File Reference . . . . .	395
11.12manifest.py File Reference . . . . .	395
11.13oids.py File Reference . . . . .	396
11.14pubd.py File Reference . . . . .	396
11.15publication.py File Reference . . . . .	397
11.16relaxng.py File Reference . . . . .	397
11.17resource_set.py File Reference . . . . .	398
11.18roa.py File Reference . . . . .	399
11.19rootd.py File Reference . . . . .	399
11.20rpki_engine.py File Reference . . . . .	401
11.21rpkid.py File Reference . . . . .	401
11.22sql.py File Reference . . . . .	401
11.23sundial.py File Reference . . . . .	402
11.24up_down.py File Reference . . . . .	402
11.25x509.py File Reference . . . . .	403
11.26xml_utils.py File Reference . . . . .	403

## 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`
- <http://trevp.net/tlslite/>. `TLSLite` pulls in other crypto packages.
  - FreeBSD: `/usr/ports/security/py-tlsLite`

`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 `xsltproc`, 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 rpkiid's own database, using the left-right control protocol.
- `cronjob.py`: A trivial HTTP client used to drive `rpkiid` cron events.
- `testbed.py`: A test tool for running a collection of `rpkiid` and `irdb` instances under common control, driven by a unified test script.
- `testpoke.py`: A simple client for the up-down protocol, mostly compatible with APNIC's `rpki_poke.pl` tool.

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

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

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

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

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

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

## 4.1 rpkiid.py

`rpkiid` is the main RPKI engine daemon. Configuration of `rpkiid` is a two step process: a config file to bootstrap `rpkiid` to the point where it can speak using the `left-right protocol`,

followed by dynamic configuration via the left-right protocol. In production use the latter stage would be handled by the IRBE stub; for test and development purposes it's handled by the [irbe\\_cli.py](#) command line interface or by the [testbed.py](#) test framework.

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

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

Config file options:

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

## 4.5 irbe\_cli.py

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

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

At present the user is assumed to be able to read the (XML) left-right and [publication](#) protocol messages, and with one exception, irdbd-cli makes no attempt to interpret the responses other than to check for signature and syntax errors. The one exception is that, if the `-pem_out` option is specified on the command line, any PKCS #10 requests received from [rpki](#) 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 rpki 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](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.

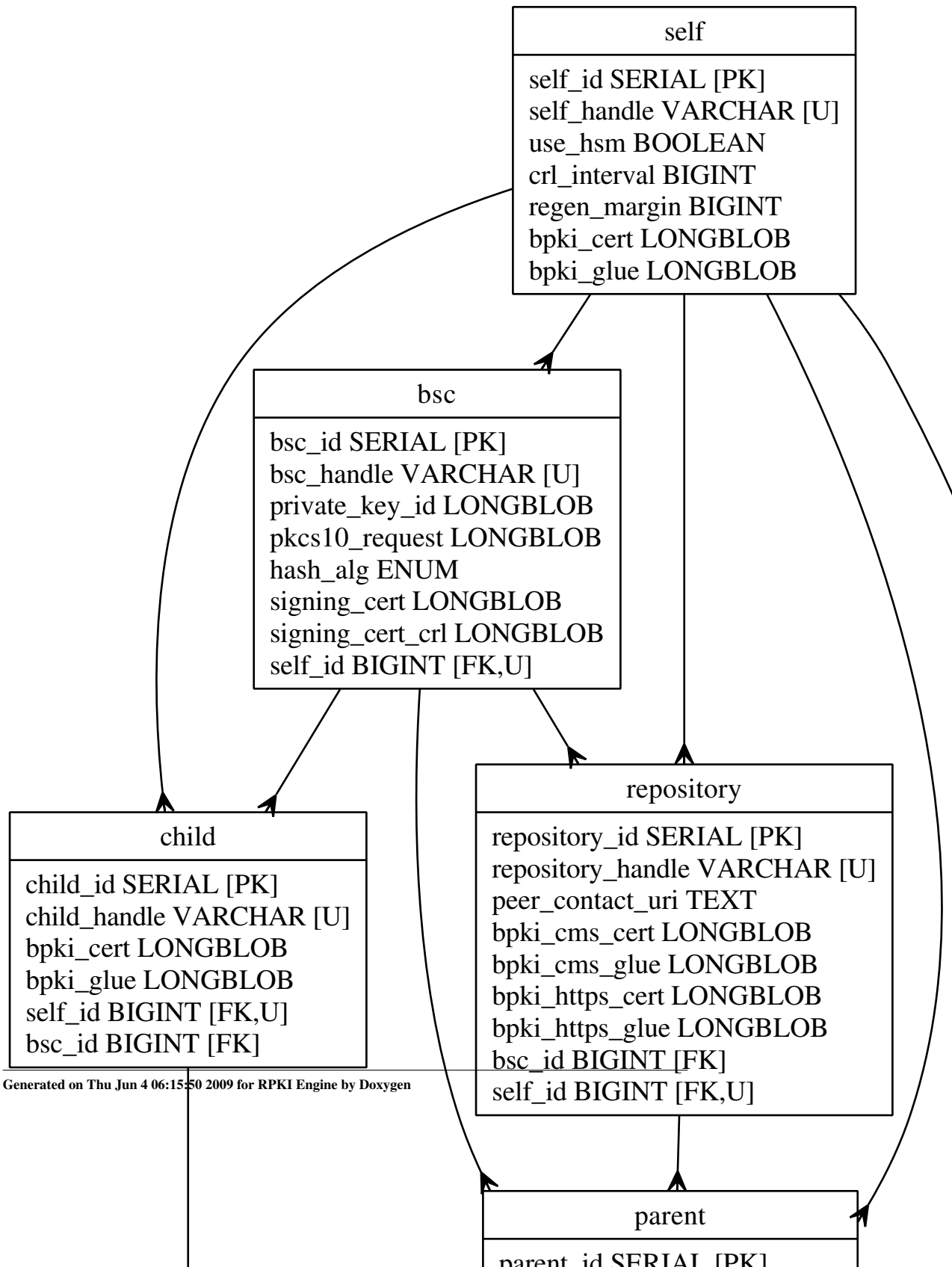
## 7 SQL database schemas

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





## 7.1 rpkiid SQL schema



```
-- $Id: rpkiid.sql 2491 2009-06-03 05:07:04Z 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 IF EXISTS self;

CREATE TABLE self (
    self_id          SERIAL NOT NULL,
    self_handle      VARCHAR(255) NOT NULL,
    use_hsm          BOOLEAN,
    crl_interval     BIGINT unsigned,
    regen_margin     BIGINT unsigned,
    bpki_cert        LONGBLOB,
    bpki_glue        LONGBLOB,
    PRIMARY KEY      (self_id),
    UNIQUE           (self_handle)
);

DROP TABLE IF EXISTS bsc;

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,
    UNIQUE           (self_id, bsc_handle)
);

DROP TABLE IF EXISTS repository;

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,
```

```

        bпки_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,
        FOREIGN KEY               (bsc_id) REFERENCES bsc,
        UNIQUE                    (self_id, repository_handle)
);

DROP TABLE IF EXISTS parent;

CREATE TABLE parent (
    parent_id                    SERIAL NOT NULL,
    parent_handle                VARCHAR(255) NOT NULL,
    bпки_cms_cert                LONGBLOB,
    bпки_https_glue              LONGBLOB,
    bпки_https_cert              LONGBLOB,
    bпки_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,
    FOREIGN KEY                  (bsc_id) REFERENCES bsc,
    FOREIGN KEY                  (self_id) REFERENCES self,
    UNIQUE                      (self_id, parent_handle)
);

DROP TABLE IF EXISTS ca;

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
);

DROP TABLE IF EXISTS ca_detail;

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

```

```

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

DROP TABLE IF EXISTS child;

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

DROP TABLE IF EXISTS child_cert;

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,
    FOREIGN KEY              (child_id) REFERENCES child
);

DROP TABLE IF EXISTS revoked_cert;

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
);

DROP TABLE IF EXISTS route_origin;

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,
        FOREIGN KEY                        (ca_detail_id) REFERENCES ca_detail,
        UNIQUE                             (self_id, route_origin_handle)
    );

DROP TABLE IF EXISTS route_origin_prefix;

CREATE TABLE route_origin_prefix (
    address                                VARCHAR(40) NOT NULL,
    prefixlen                             TINYINT NOT NULL,
    max_prefixlen                         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
);

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

```

## 7.2 pubd SQL Schema

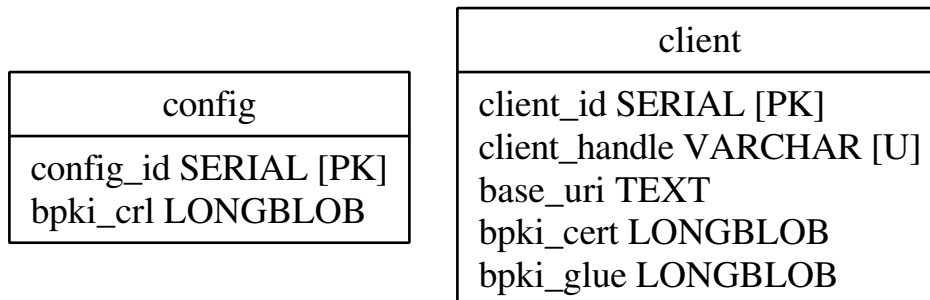


Figure 2: Diagram of pubd.sql

```

-- $Id: pubd.sql 1835 2008-06-02 23:43:01Z 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 config;  
  
CREATE TABLE config (  
    config_id      SERIAL NOT NULL,  
    bpki_crl       LONGBLOB,  
    PRIMARY KEY    (config_id)  
);  
  
DROP TABLE IF EXISTS client;  
  
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)  
);  
  
-- Local Variables:  
-- indent-tabs-mode: nil  
-- End:
```

## 7.3 irdbd SQL Schema

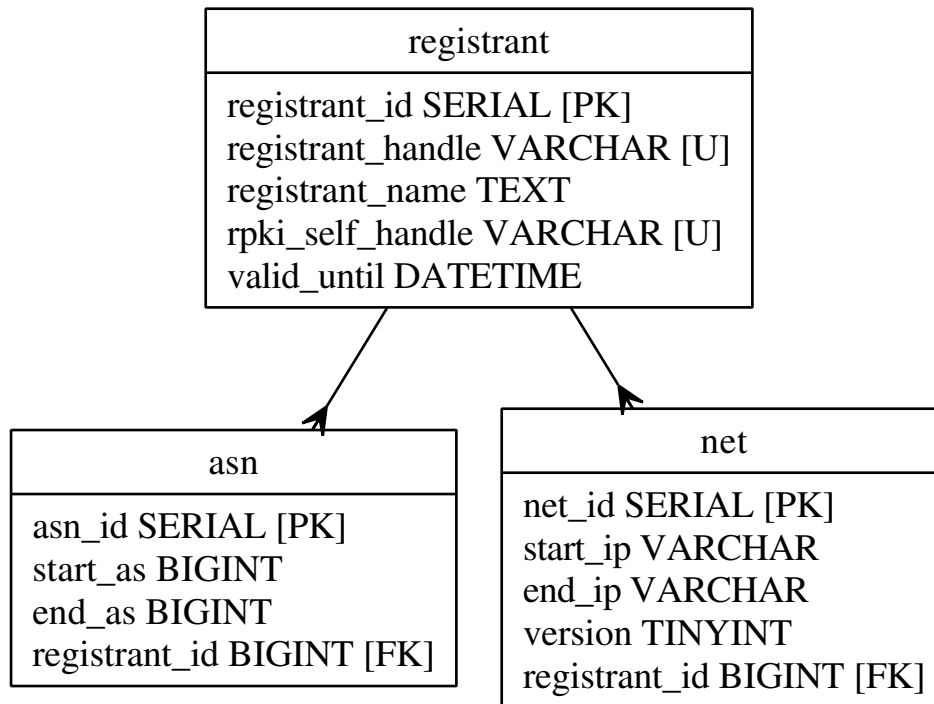


Figure 3: Diagram of irdbd.sql

```

-- $Id: irdbd.sql 2491 2009-06-03 05:07:04Z 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 IF EXISTS registrant;

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

DROP TABLE IF EXISTS asn;

CREATE TABLE asn (
    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        (asn_id),
    FOREIGN KEY        (registrant_id) REFERENCES registrant ON DELETE SET NULL ON UPDATE SET NULL
);

DROP TABLE IF EXISTS net;

CREATE TABLE net (
    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        (net_id),
    FOREIGN KEY        (registrant_id) REFERENCES registrant ON DELETE SET NULL ON UPDATE SET NULL
);

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

```

## 8 BPKI model

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

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

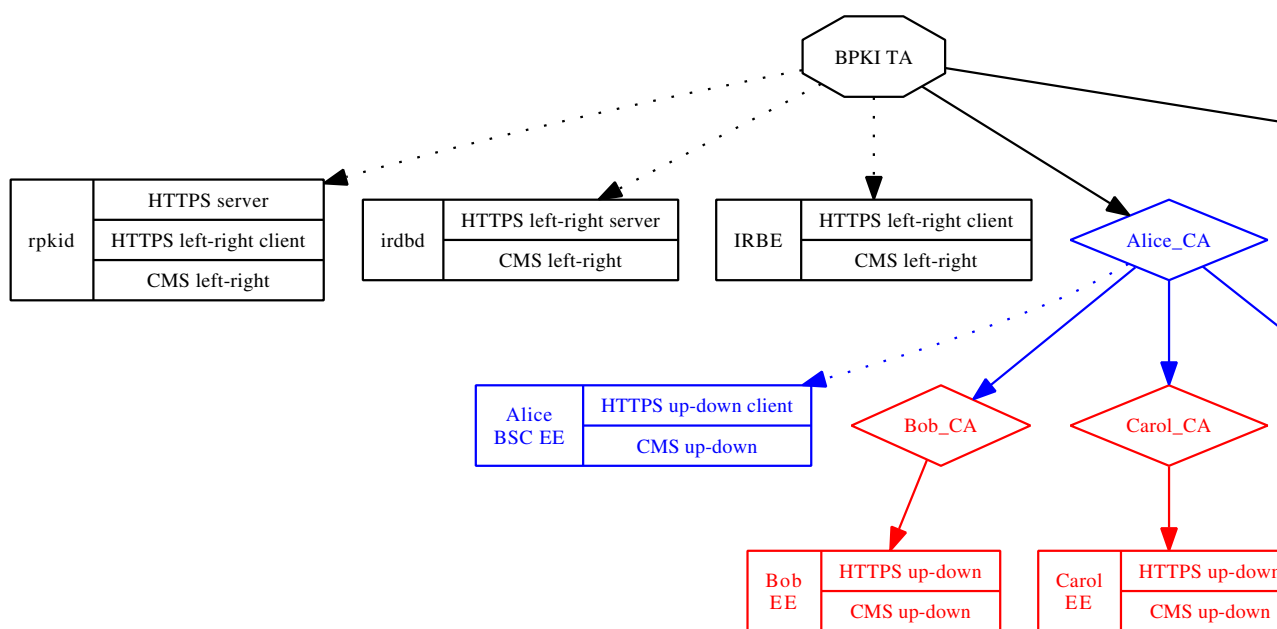
Setup of the BPKI is handled by the back end; for the most part, [rpkid](#) and [pubd](#) just use the result. The one place where the engines are directly involved in creation of new BPKI certificates is in the production of end-entity certificates for use by the engines.

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

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

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

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



Black objects belong to the hosting entity, blue objects belong to the hosted entities, red objects are cross-certified objects from the hosted entities' peers. The arrows indicate certificate issuance: solid arrows are the ones that rpkid will care about during

certificate validation, dotted arrows show the origin of the EE certificates that [rpkid](#) uses to sign CMS and TLS messages.

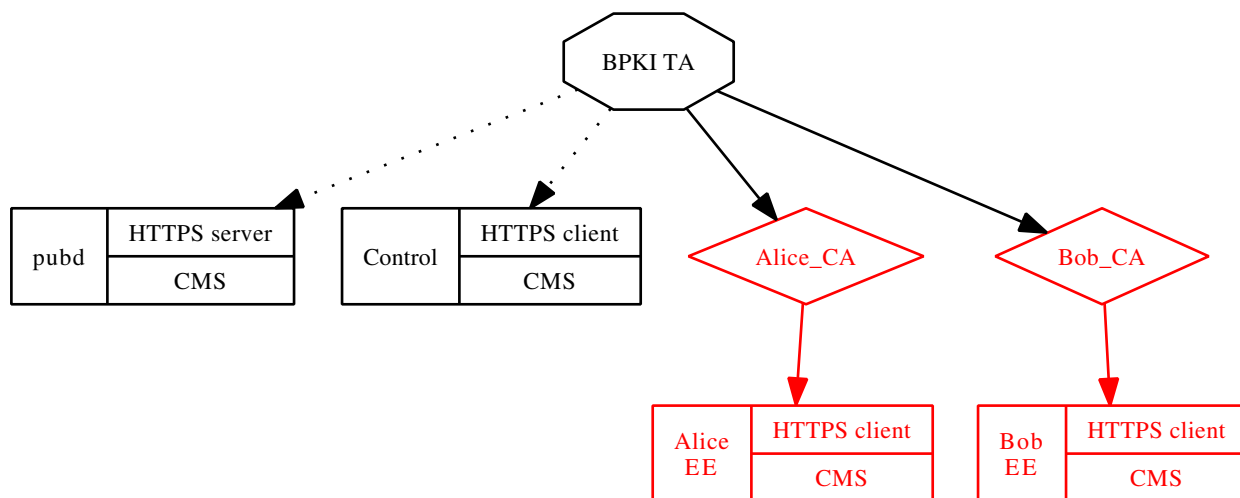
There's one nasty bit where the model had to bend to fit the current state of the underlying protocols: it's not possible to use exactly the same BPKI keys and certificates for HTTPS and CMS. The reason for this is simple: each hosted entity has its own BPKI, as does the hosting entity, but the HTTPS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

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

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

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

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



While it is likely that RIRs (at least) will operate both [rpkid](#) 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 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.

### 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 2491 2009-06-03 05:07:04Z 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 132 of file irdbd.py.

#### 9.3.3.2 tuple irdbd.cfg = rpki.config.parser(cfg\_file, "irdbd")

Definition at line 120 of file irdbd.py.

#### 9.3.3.3 irdbd.cfg\_file = "irdbd.conf"

Definition at line 108 of file irdbd.py.

#### 9.3.3.4 tuple irdbd.client\_ta = (bpki\_ta, rpkiid\_cert)

Definition at line 148 of file irdbd.py.

#### 9.3.3.5 tuple irdbd.cur = db.cursor()

Definition at line 130 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 126 of file irdbd.py.

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

Definition at line 151 of file irdbd.py.

#### **9.3.3.8 string irdbd.host = "localhost"**

Definition at line 149 of file irdbd.py.

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

Definition at line 134 of file irdbd.py.

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

Definition at line 135 of file irdbd.py.

#### **9.3.3.11 int irdbd.port = 443**

Definition at line 150 of file irdbd.py.

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

Definition at line 133 of file irdbd.py.

**9.3.3.13** `irdbd.server_cert = irdbd_cert,`

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

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

Definition at line 122 of file `irdbd.py`.

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

Definition at line 137 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 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.

## 9.4.2 Function Documentation

### 9.4.2.1 def pubd.main ()

Definition at line 168 of file pubd.py.

## 9.4.3 Variable Documentation

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

Definition at line 153 of file pubd.py.

### 9.4.3.2 pubd.profile = False

Definition at line 154 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 [ipaddrs](#)
- package [left\\_right](#)
- package [log](#)
- package [manifest](#)
- package [oids](#)
- package [publication](#)
- package [relaxng](#)
- package [resource\\_set](#)
- package [roa](#)
- package [rpki\\_engine](#)
- package [sql](#)
- package [sundial](#)
- package [up\\_down](#)
- package [x509](#)
- package [xml\\_utils](#)

## 9.7 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 [DBConsistancyError](#)
- 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 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.

## 9.10 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 2486 2009-06-02 03:09:43Z 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 [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 2491 2009-06-03 05:07:04Z 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 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.

### 9.16.2 Variable Documentation

#### 9.16.2.1 `rpki::publication::obj2elt = dict((e.payload_type, e) for e in (certificate_elt, crt_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 1227 of file relaxng.py.

#### 9.17.1.3 rpki::relaxng::up\_down

Parsed RelaxNG [up\\_down](#) schema.

Definition at line 973 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 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.

## 9.21 Package rpki.sql

### Classes

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

### 9.21.1 Detailed Description

SQL interface code.

\$Id: sql.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 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 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.

### 9.23.2 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 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.

### 9.24.2 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 681 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 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 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 rpkiid.main ()

Definition at line 66 of file rpkiid.py.

## 9.26.3 Variable Documentation

### 9.26.3.1 rpkiid.cfg\_file = "rpkiid.conf"

Definition at line 51 of file rpkiid.py.

### 9.26.3.2 `rpkiid.profile = None`

Definition at line 52 of file `rpkiid.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 \(2486\)](#)

### 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 \(2486\)](#)

### 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 \(2452\)](#)

### 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_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, crt_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](#) (2481)

## 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

- [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 136 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 128 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 96 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 `pubd.pubd_context.https_server_host`

Definition at line 60 of file pubd.py.

### 10.28.3.3 `pubd.pubd_context.https_server_port`

Definition at line 61 of file pubd.py.

### 10.28.3.4 `pubd.pubd_context::https_ta_cache = None` `[static]`

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

Definition at line 126 of file pubd.py.

### 10.28.3.5 `pubd.pubd_context.irbe_cert`

Definition at line 56 of file pubd.py.

### 10.28.3.6 pubd.pubd\_context.pubd\_cert

Definition at line 57 of file pubd.py.

### 10.28.3.7 pubd.pubd\_context.pubd\_key

Definition at line 58 of file pubd.py.

### 10.28.3.8 pubd.pubd\_context.publication\_base

Definition at line 63 of file pubd.py.

### 10.28.3.9 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 \(2481\)](#)

## 10.29 pydatetime.datetime Class Reference

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

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

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

## 10.30 pydatetime.timedelta Class Reference

Inherited by [rpk.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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 10.60 rpki.exceptions.DEROObjectConversionError 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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.CMSCRLNotSet](#),  
[rpki.exceptions.CMSVerificationFailed](#), [rpki.exceptions.DBConsistencyError](#),  
[rpki.exceptions.DERObjectConversionError](#), [rpki.exceptions.DuplicateObject](#),  
[rpki.exceptions.EmptyPEM](#), [rpki.exceptions.ForbiddenURI](#),  
[rpki.exceptions.HTTPRequestFailed](#), [rpki.exceptions.HTTPSClientAborted](#),  
[rpki.exceptions.MissingCMSCRL](#), [rpki.exceptions.MissingCMSEECert](#),  
[rpki.exceptions.MustBePrefix](#), [rpki.exceptions.NoActiveCA](#),  
[rpki.exceptions.NotACertificateChain](#), [rpki.exceptions.NotFound](#),  
[rpki.exceptions.NotImplementedYet](#), [rpki.exceptions.NotInDatabase](#),  
[rpki.exceptions.ServerShuttingDown](#), [rpki.exceptions.SKIMismatch](#),  
[rpki.exceptions.SubprocessError](#), [rpki.exceptions.TLSValidationError](#),  
[rpki.exceptions.UnexpectedCMSCerts](#), [rpki.exceptions.UnexpectedCMSCRLs](#),  
[rpki.exceptions.UnparsableCMSDER](#), [rpki.exceptions.UpstreamError](#), and  
[rpki.exceptions.WrongEContentType](#).

### 10.76.1 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)



## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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 \(2452\)](#)

## 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](#) (2486)

## 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 \(2486\)](#)

## 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 \(2486\)](#)

## 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 \(2486\)](#)

## 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 \(2486\)](#)

## 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 \(2486\)](#)

## 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](#) (2486)

### 10.93 `rpki.https.http_stream` Class Reference

Inherits [asynchat::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 \(2486\)](#)

## 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.*
- [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 405 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 435 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 431 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 427 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 439 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 411 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 413 of file `left_right.py`.

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

Definition at line 410 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 412 of file `left_right.py`.

**10.96.3.5** `rpki.left_right.bsc_elt.pkcs10_request = None [static]`

Definition at line 423 of file `left_right.py`.

**10.96.3.6** `rpki.left_right.bsc_elt.private_key_id = None [static]`

Definition at line 422 of file `left_right.py`.

**10.96.3.7** `rpki.left_right.bsc_elt.signing_cert = None [static]`

Reimplemented in [irbe\\_cli.bsc\\_elt](#).

Definition at line 424 of file `left_right.py`.

### 10.96.3.8 rpki.left\_right.bsc\_elt.signing\_cert\_crl = None [static]

Reimplemented in [irbe\\_cli.bsc\\_elt](#).

Definition at line 425 of file left\_right.py.

### 10.96.3.9 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 415 of file left\_right.py.

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

- [left\\_right.py \(2491\)](#)

## 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 `sql_template`

### 10.97.1 Detailed Description

`<child/>` element.

Definition at line 551 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 578 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 570 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 602 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 574 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 592 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 612 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 557 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 559 of file left\_right.py.

#### 10.97.3.3 rpki.left\_right.child\_elt.bpki\_cert = None [static]

Definition at line 566 of file left\_right.py.

#### 10.97.3.4 rpki.left\_right.child\_elt.bpki\_glue = None [static]

Definition at line 567 of file left\_right.py.

#### 10.97.3.5 rpki.left\_right.child\_elt.clear\_https\_ta\_cache = False [static]

Definition at line 568 of file left\_right.py.

#### 10.97.3.6 string rpki.left\_right.child\_elt.element\_name = "child" [static]

Definition at line 556 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 558 of file left\_right.py.

### 10.97.3.8 tuple rpki.left\_right.child\_elt.sql\_template [static]

#### Initial value:

```
rpki.sql.template("child", "child_id", "child_handle",  
                  "self_id", "bsc_id",  
                  ("bpki_cert", rpki.x509.X509),  
                  ("bpki_glue", rpki.x509.X509))
```

Definition at line 561 of file left\_right.py.

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

- [left\\_right.py](#) (2491)

## 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 1094 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 1099 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 1101 of file `left_right.py`.

### 10.98.2.3 rpki.left\_right.cms\_msg.schema = rpki.relaxng.left\_right [static]

Definition at line 1100 of file `left_right.py`.

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

- [left\\_right.py](#) (2491)

## 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\\_one\\_maybe](#)
- def [serve\\_pre\\_save\\_hook](#)
- def [unimplemented\\_control](#)

### Public Attributes

- [self\\_id](#)

### 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 60 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 64 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 56 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 77 of file left\_right.py.

### 10.99.2.5 `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 68 of file left\_right.py.

### 10.99.2.6 `def rpki.left_right.data_elt.serve_pre_save_hook ( self, q_pdu, r_pdu, cb, eb)`

Hook to set self\_id properly before saving.

Reimplemented from [rpki.xml\\_utils.data\\_elt](#).

Reimplemented in [rpki.left\\_right.self\\_elt](#), and [rpki.left\\_right.bsc\\_elt](#).

Definition at line 84 of file left\_right.py.

### 10.99.2.7 `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 96 of file left\_right.py.

## 10.99.3 Member Data Documentation

### 10.99.3.1 `rpki.left_right.data_elt.self_id`

Reimplemented in [rpki.left\\_right.self\\_elt](#).

Definition at line 93 of file left\_right.py.

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

- [left\\_right.py \(2491\)](#)

## 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.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](#) (2491)

## 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 989 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 998 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 1014 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 1008 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 995 of file left\_right.py.

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

Definition at line 994 of file left\_right.py.

**10.101.3.4 rpki.left\_right.list\_resources\_elt.ipv4**

Definition at line 1010 of file left\_right.py.

### 10.101.3.5 rpki.left\_right.list\_resources\_elt.ipv6

Definition at line 1012 of file left\_right.py.

### 10.101.3.6 rpki.left\_right.list\_resources\_elt.valid\_until = None [static]

Definition at line 996 of file left\_right.py.

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

- [left\\_right.py \(2491\)](#)

## 10.102 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.*

### 10.102.1 Detailed Description

Left-right PDU.

Definition at line 1043 of file left\_right.py.

## 10.102.2 Member Function Documentation

### 10.102.2.1 def rpki.left\_right.msg.serve\_top\_level ( self, gctx, cb)

Serve one msg PDU.

Definition at line 1058 of file left\_right.py.

## 10.102.3 Member Data Documentation

### 10.102.3.1 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, report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented in [irbe\\_cli.left\\_right\\_msg](#).

Definition at line 1054 of file left\_right.py.

### 10.102.3.2 rpki::left\_right.msg::version = 1 [static]

Protocol version.

Reimplemented from [rpki.xml\\_utils.msg](#).

Definition at line 1050 of file left\_right.py.

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

- [left\\_right.py \(2491\)](#)

## 10.103 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 [sql\\_template](#)

### 10.103.1 Detailed Description

`<parent/> element.`

Definition at line 452 of file `left_right.py`.

### 10.103.2 Member Function Documentation

#### 10.103.2.1 def rpki.left\_right.parent\_elt.cas ( self)

Fetch all CA objects that link to this parent object.

Definition at line 478 of file `left_right.py`.

**10.103.2.2** `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 514 of file left\_right.py.

**10.103.2.3** `def rpki.left_right.parent_elt.repository ( self)`

Fetch repository object to which this parent object links.

Definition at line 474 of file left\_right.py.

**10.103.2.4** `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 482 of file left\_right.py.

**10.103.2.5** `def rpki.left_right.parent_elt.serve_rekey ( self, cb, eb)`

Handle a left-right rekey action for this parent.

Definition at line 494 of file left\_right.py.

**10.103.2.6** `def rpki.left_right.parent_elt.serve_revoke ( self, cb, eb)`

Handle a left-right revoke action for this parent.

Definition at line 504 of file left\_right.py.

### 10.103.3 Member Data Documentation

#### 10.103.3.1 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 458 of file `left_right.py`.

#### 10.103.3.2 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 461 of file `left_right.py`.

#### 10.103.3.3 `rpki.left_right.parent_elt.bpki_cms_cert` = None [static]

Definition at line 469 of file `left_right.py`.

#### 10.103.3.4 `rpki.left_right.parent_elt.bpki_cms_glue` = None [static]

Definition at line 470 of file `left_right.py`.

#### 10.103.3.5 `rpki.left_right.parent_elt.bpki_https_cert` = None [static]

Definition at line 471 of file `left_right.py`.

**10.103.3.6** `rpki.left_right.parent_elt.bpki_https_glue = None` `[static]`

Definition at line 472 of file left\_right.py.

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

Definition at line 457 of file left\_right.py.

**10.103.3.8** `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 460 of file left\_right.py.

**10.103.3.9** `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 463 of file left\_right.py.

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

- [left\\_right.py \(2491\)](#)

**10.104** `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"

### 10.104.1 Detailed Description

<report\_error/> element.

Definition at line 1024 of file left\_right.py.

### 10.104.2 Member Function Documentation

#### 10.104.2.1 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 1033 of file left\_right.py.

### 10.104.3 Member Data Documentation

#### 10.104.3.1 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 1030 of file left\_right.py.

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

Definition at line 1029 of file left\_right.py.

**10.104.3.3** `rpki.left_right.report_error_elt.error_code`

Definition at line 1039 of file left\_right.py.

**10.104.3.4** `rpki.left_right.report_error_elt.self_handle`

Definition at line 1038 of file left\_right.py.

**10.104.3.5** `rpki.left_right.report_error_elt.text`

Definition at line 1040 of file left\_right.py.

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

- [left\\_right.py \(2491\)](#)

## 10.105 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 `sql_template`

#### 10.105.1 Detailed Description

<repository/> element.

Definition at line 649 of file left\_right.py.

#### 10.105.2 Member Function Documentation

##### 10.105.2.1 `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 672 of file left\_right.py.

##### 10.105.2.2 `def rpki.left_right.repository_elt.parents (self)`

Fetch all parent objects that link to this repository object.

Definition at line 668 of file left\_right.py.

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

Publish one object in the repository.

Definition at line 703 of file left\_right.py.

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

Withdraw one object from the repository.

Definition at line 711 of file left\_right.py.

**10.105.3 Member Data Documentation****10.105.3.1** `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 655 of file left\_right.py.

**10.105.3.2** `rpki.left_right.repository_elt.bpki_cms_cert = None [static]`

Definition at line 663 of file left\_right.py.

**10.105.3.3** `rpki.left_right.repository_elt.bpki_cms_glue = None [static]`

Definition at line 664 of file left\_right.py.

**10.105.3.4 rpki.left\_right.repository\_elt.bpki\_https\_cert = None** [static]

Definition at line 665 of file left\_right.py.

**10.105.3.5 rpki.left\_right.repository\_elt.bpki\_https\_glue = None** [static]

Definition at line 666 of file left\_right.py.

**10.105.3.6 string rpki.left\_right.repository\_elt.element\_name = "repository"**  
[static]

Definition at line 654 of file left\_right.py.

**10.105.3.7 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 656 of file left\_right.py.

**10.105.3.8 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 658 of file left\_right.py.

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

- [left\\_right.py \(2491\)](#)

## 10.106 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"
- [publish\\_ee\\_separately](#) = False

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

- `roa` = None
- tuple `sql_template`

### 10.106.1 Detailed Description

`<route_origin/>` element.

Definition at line 719 of file `left_right.py`.

### 10.106.2 Member Function Documentation

#### 10.106.2.1 `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 779 of file `left_right.py`.

#### 10.106.2.2 `def rpki.left_right.route_origin_elt.ee_uri ( self, ca)`

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

Definition at line 985 of file `left_right.py`.

#### 10.106.2.3 `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 981 of file `left_right.py`.

#### 10.106.2.4 `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 847 of file left\_right.py.

#### 10.106.2.5 `def rpki.left_right.route_origin_elt.regenerate_roa ( self, callback, errback)`

Reissue ROA associated with this route\_origin.

Definition at line 964 of file left\_right.py.

#### 10.106.2.6 `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 973 of file left\_right.py.

#### 10.106.2.7 `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 977 of file left\_right.py.



**10.106.2.8** `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 783 of file left\_right.py.

**10.106.2.9** `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 772 of file left\_right.py.

**10.106.2.10** `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 741 of file left\_right.py.

**10.106.2.11** `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 758 of file left\_right.py.

**10.106.2.12** `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 790 of file left\_right.py.

**10.106.2.13** `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 804 of file left\_right.py.

**10.106.2.14** `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 922 of file left\_right.py.

**10.106.3 Member Data Documentation****10.106.3.1** `rpki.left_right.route_origin_elt.as_number`

Reimplemented in [irbe\\_cli.route\\_origin\\_elt](#).

Definition at line 798 of file left\_right.py.

**10.106.3.2** `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 725 of file `left_right.py`.

**10.106.3.3** `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 726 of file `left_right.py`.

**10.106.3.4** `rpki.left_right.route_origin_elt.ca_detail_id = None [static]`

Definition at line 733 of file `left_right.py`.

**10.106.3.5** `rpki.left_right.route_origin_elt.cert = None [static]`

Definition at line 734 of file `left_right.py`.

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

Definition at line 724 of file `left_right.py`.

**10.106.3.7** `rpki.left_right.route_origin_elt.ipv4`

Reimplemented in [irbe\\_cli.route\\_origin\\_elt](#).

Definition at line 745 of file left\_right.py.

### 10.106.3.8 rpki.left\_right.route\_origin\_elt.ipv6

Reimplemented in [irbe\\_cli.route\\_origin\\_elt](#).

Definition at line 751 of file left\_right.py.

### 10.106.3.9 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 739 of file left\_right.py.

### 10.106.3.10 rpki.left\_right.route\_origin\_elt.roa = None [static]

Definition at line 735 of file left\_right.py.

### 10.106.3.11 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 728 of file left\_right.py.

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

- [left\\_right.py \(2491\)](#)

## 10.107 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"

#### 10.107.1 Detailed Description

SAX handler for Left-Right protocol.

Definition at line 1085 of file [left\\_right.py](#).

#### 10.107.2 Member Data Documentation

##### 10.107.2.1 string [rpki.left\\_right.sax\\_handler.name](#) = "msg" [static]

Definition at line 1091 of file [left\\_right.py](#).

##### 10.107.2.2 [rpki.left\\_right.sax\\_handler.pdu](#) = [msg](#) [static]

Reimplemented in [irbe\\_cli.left\\_right\\_sax\\_handler](#).

Definition at line 1090 of file [left\\_right.py](#).

##### 10.107.2.3 string [rpki.left\\_right.sax\\_handler.version](#) = "1" [static]

Definition at line 1092 of file [left\\_right.py](#).

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

- [left\\_right.py](#) (2491)

### 10.108 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\\_pre\\_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.*

- [regen\\_margin](#) = None
- [self\\_id](#) = None
- tuple [sql\\_template](#)
- [use\\_hsm](#) = False

### 10.108.1 Detailed Description

`<self/> element.`

Definition at line 104 of file left\_right.py.

### 10.108.2 Member Function Documentation

#### 10.108.2.1 `def rpki.left_right.self_elt.bscs ( self )`

Fetch all BSC objects that link to this self object.

Definition at line 125 of file left\_right.py.

#### 10.108.2.2 `def rpki.left_right.self_elt.children ( self )`

Fetch all child objects that link to this self object.

Definition at line 137 of file left\_right.py.

#### 10.108.2.3 `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 208 of file left\_right.py.

#### 10.108.2.4 `def rpki.left_right.self_elt.parents ( self )`

Fetch all parent objects that link to this self object.

Definition at line 133 of file left\_right.py.

**10.108.2.5 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 343 of file left\_right.py.

**10.108.2.6 def rpki.left\_right.self\_elt.repositories ( self)**

Fetch all repository objects that link to this self object.

Definition at line 129 of file left\_right.py.

**10.108.2.7 def rpki.left\_right.self\_elt.route\_origins ( self)**

Fetch all route\_origin objects that link to this self object.

Definition at line 141 of file left\_right.py.

**10.108.2.8 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 194 of file left\_right.py.



**10.108.2.9** `def rpki.left_right.self_elt.serve_fetch_handle ( cls, gctx,  
self_handle)`

Find a `self` object based on its `self_handle`.

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

**10.108.2.10** `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 180 of file `left_right.py`.

**10.108.2.11** `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 145 of file `left_right.py`.

**10.108.2.12** `def rpki.left_right.self_elt.serve_pre_save_hook ( self, q_pdu,  
r_pdu, cb, eb)`

Override hook back to no-op (override of `override`).

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

Definition at line 202 of file `left_right.py`.

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

Handle a left-right rekey action for this self.

Definition at line 158 of file left\_right.py.

**10.108.2.14** `def rpki.left_right.self_elt.serve_revoke ( self, cb, eb)`

Handle a left-right revoke action for this self.

Definition at line 169 of file left\_right.py.

**10.108.2.15** `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 261 of file left\_right.py.

**10.108.2.16** `def rpki.left_right.self_elt.update_roas ( self, cb)`

Generate or update ROAs for this self's route\_origin objects.

Definition at line 394 of file left\_right.py.

**10.108.3 Member Data Documentation****10.108.3.1** `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 110 of file left\_right.py.

**10.108.3.2** `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 112 of file left\_right.py.

**10.108.3.3** `rpki.left_right.self_elt.bpki_cert = None [static]`

Definition at line 122 of file left\_right.py.

**10.108.3.4** `rpki.left_right.self_elt.bpki_glue = None [static]`

Definition at line 123 of file left\_right.py.

**10.108.3.5** `rpki.left_right.self_elt.crl_interval = None [static]`

Definition at line 120 of file left\_right.py.

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

Definition at line 109 of file left\_right.py.

**10.108.3.7** `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 111 of file left\_right.py.

**10.108.3.8 rpki.left\_right.self\_elt.regen\_margin = None** [static]

Definition at line 121 of file left\_right.py.

**10.108.3.9 rpki.left\_right.self\_elt.self\_id = None** [static]

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

Definition at line 118 of file left\_right.py.

**10.108.3.10 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 114 of file left\_right.py.

**10.108.3.11 rpki.left\_right.self\_elt.use\_hsm = False** [static]

Definition at line 119 of file left\_right.py.

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

- [left\\_right.py \(2491\)](#)

**10.109 rpki.log.logger Class Reference**

Inherits [object](#).

**Public Member Functions**

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

## Public Attributes

- [priority](#)

### 10.109.1 Detailed Description

Closure for logging.

Definition at line 70 of file log.py.

### 10.109.2 Member Function Documentation

#### 10.109.2.1 def rpki.log.logger.\_\_call\_\_ ( *self*, *message* )

Definition at line 78 of file log.py.

#### 10.109.2.2 def rpki.log.logger.\_\_init\_\_ ( *self*, *priority* )

Definition at line 75 of file log.py.

### 10.109.3 Member Data Documentation

#### 10.109.3.1 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 \(2452\)](#)

## 10.110 rpki.manifest.FileAndHash Class Reference

Inherits [Sequence](#).

## Public Member Functions

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

## Public Attributes

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

### 10.110.1 Detailed Description

Definition at line 27 of file manifest.py.

### 10.110.2 Member Function Documentation

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

Definition at line 28 of file manifest.py.

### 10.110.3 Member Data Documentation

#### 10.110.3.1 rpki.manifest.FileAndHash.file

Definition at line 29 of file manifest.py.

#### 10.110.3.2 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 \(2424\)](#)

## 10.111 rpki.manifest.FilesAndHashes Class Reference

Inherits [SequenceOf](#).

## Public Member Functions

- `def __init__`

### 10.111.1 Detailed Description

Definition at line 34 of file manifest.py.

### 10.111.2 Member Function Documentation

#### 10.111.2.1 `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 \(2424\)](#)

## 10.112 rpki.manifest.Manifest Class Reference

Inherits [Sequence](#).

### Public Member Functions

- `def __init__`

### Public Attributes

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

### 10.112.1 Detailed Description

Definition at line 38 of file manifest.py.

### 10.112.2 Member Function Documentation

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

Definition at line 39 of file manifest.py.

### 10.112.3 Member Data Documentation

#### 10.112.3.1 `rpki.manifest.Manifest.explicitVersion`

Definition at line 41 of file manifest.py.

#### 10.112.3.2 `rpki.manifest.Manifest.fileHashAlg`

Definition at line 45 of file manifest.py.

#### 10.112.3.3 `rpki.manifest.Manifest.fileList`

Definition at line 46 of file manifest.py.

#### 10.112.3.4 `rpki.manifest.Manifest.manifestNumber`

Definition at line 42 of file manifest.py.

#### 10.112.3.5 `rpki.manifest.Manifest.nextUpdate`

Definition at line 44 of file manifest.py.

#### 10.112.3.6 `rpki.manifest.Manifest.thisUpdate`

Definition at line 43 of file manifest.py.



### 10.112.3.7 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 \(2424\)](#)

## 10.113 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](#)

### 10.113.1 Detailed Description

<certificate/> element.

Definition at line 245 of file publication.py.

### 10.113.2 Member Data Documentation

#### 10.113.2.1 string rpki.publication.certificate\_elt.element\_name = "certificate" [static]

Definition at line 250 of file publication.py.

#### 10.113.2.2 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 \(2481\)](#)

## 10.114 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](#)))

### 10.114.1 Detailed Description

<client/> element.

Definition at line 113 of file publication.py.

### 10.114.2 Member Function Documentation

#### 10.114.2.1 def rpki.publication.client\_elt.check\_allowed\_uri ( self, uri)

Definition at line 160 of file publication.py.

**10.114.2.2 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.

**10.114.2.3 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.

**10.114.2.4 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.

**10.114.2.5 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.

### 10.114.3 Member Data Documentation

**10.114.3.1** `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`.

**10.114.3.2** `rpki.publication.client_elt.base_uri = None [static]`

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

**10.114.3.3** `rpki.publication.client_elt.bpki_cert = None [static]`

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

**10.114.3.4** `rpki.publication.client_elt.bpki_glue = None [static]`

Definition at line 126 of file `publication.py`.

**10.114.3.5** `rpki.publication.client_elt.clear_https_ta_cache = False [static]`

Definition at line 128 of file `publication.py`.

**10.114.3.6** `string rpki.publication.client_elt.element_name = "client" [static]`

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

**10.114.3.7** 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`.

**10.114.3.8** 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](#) (2481)

## 10.115 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`

### 10.115.1 Detailed Description

Class to hold a CMS-signed publication PDU.

Definition at line 352 of file `publication.py`.

### 10.115.2 Member Data Documentation

#### 10.115.2.1 string rpki.publication.cms\_msg.encoding = "us-ascii" [static]

Definition at line 357 of file publication.py.

#### 10.115.2.2 rpki.publication.cms\_msg.saxify = sax\_handler.saxify [static]

Reimplemented in [irbe\\_cli.publication\\_cms\\_msg](#).

Definition at line 359 of file publication.py.

#### 10.115.2.3 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](#) (2481)

## 10.116 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

#### 10.116.1 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`.

#### 10.116.2 Member Function Documentation

##### 10.116.2.1 `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`.

##### 10.116.2.2 `def rpki.publication.config_elt.serve_fetch_one_maybe ( self )`

Find the config object on which a get or set method should operate, or which would conflict with a create method.

Definition at line 106 of file `publication.py`.

**10.116.2.3 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.

**10.116.2.4 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.

**10.116.3 Member Data Documentation****10.116.3.1 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.

**10.116.3.2 rpki.publication.config\_elt.config\_id**

Definition at line 86 of file publication.py.

**10.116.3.3 string rpki.publication.config\_elt.element\_name = "config"  
[static]**

Definition at line 73 of file publication.py.



**10.116.3.4** `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`.

**10.116.3.5** `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`.

**10.116.3.6** `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](#) (2481)

## 10.117 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](#)

### 10.117.1 Detailed Description

Virtual class for control channel objects.

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

## 10.117.2 Member Function Documentation

### 10.117.2.1 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 \(2481\)](#)

## 10.118 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](#)

### 10.118.1 Detailed Description

<crl/> element.

Definition at line 253 of file publication.py.

### 10.118.2 Member Data Documentation

#### 10.118.2.1 string rpki.publication.crl\_elt.element\_name = "crl" [static]

Definition at line 258 of file publication.py.

### 10.118.2.2 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 \(2481\)](#)

## 10.119 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](#)

### 10.119.1 Detailed Description

<manifest/> element.

Definition at line 261 of file publication.py.

### 10.119.2 Member Data Documentation

#### 10.119.2.1 string rpki.publication.manifest\_elt.element\_name = "manifest" [static]

Definition at line 266 of file publication.py.

#### 10.119.2.2 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 \(2481\)](#)

## 10.120 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.*

#### 10.120.1 Detailed Description

Publication PDU.

Definition at line 299 of file publication.py.

#### 10.120.2 Member Function Documentation

##### 10.120.2.1 def rpki.publication.msg.serve\_top\_level ( self, gctx, client, cb)

Serve one msg PDU.

Definition at line 313 of file publication.py.

#### 10.120.3 Member Data Documentation

##### 10.120.3.1 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.

### 10.120.3.2 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 \(2481\)](#)

## 10.121 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/"

### 10.121.1 Detailed Description

XML namespace parameters for publication protocol.

Definition at line 39 of file publication.py.

### 10.121.2 Member Data Documentation

#### 10.121.2.1 dictionary [rpki.publication.publication\\_namespace.nsmap](#) = { None : [xmlns](#) } [static]

Definition at line 45 of file publication.py.

```
10.121.2.2 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 \(2481\)](#)

## 10.122 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

### 10.122.1 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.

### 10.122.2 Member Function Documentation

#### 10.122.2.1 **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.

#### 10.122.2.2 **def rpki.publication.publication\_object\_elt.serve\_dispatch ( *self*, *r\_msg*, *cb*, *eb* )**

Action dispatch handler.

Definition at line 195 of file publication.py.

#### 10.122.2.3 **def rpki.publication.publication\_object\_elt.serve\_publish ( *self* )**

Publish an object.

Definition at line 214 of file publication.py.

#### 10.122.2.4 **def rpki.publication.publication\_object\_elt.serve\_withdraw ( *self* )**

Withdraw an object.

Definition at line 227 of file publication.py.

#### 10.122.2.5 **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.

#### 10.122.2.6 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.

### 10.122.3 Member Data Documentation

#### 10.122.3.1 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.

#### 10.122.3.2 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 \(2481\)](#)

### 10.123 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"

### 10.123.1 Detailed Description

`<report_error/>` element.

Definition at line 282 of file publication.py.

### 10.123.2 Member Function Documentation

#### 10.123.2.1 `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.

### 10.123.3 Member Data Documentation

#### 10.123.3.1 `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.

#### 10.123.3.2 `string rpki.publication.report_error_elt.element_name = "report_error" [static]`

Definition at line 287 of file publication.py.

### 10.123.3.3 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 \(2481\)](#)

## 10.124 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](#)

### 10.124.1 Detailed Description

<roa/> element.

Definition at line 269 of file publication.py.

### 10.124.2 Member Data Documentation

#### 10.124.2.1 string rpki.publication.roa\_elt.element\_name = "roa" [static]

Definition at line 274 of file publication.py.

#### 10.124.2.2 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 \(2481\)](#)

## 10.125 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"

### 10.125.1 Detailed Description

SAX handler for publication protocol.

Definition at line 343 of file `publication.py`.

### 10.125.2 Member Data Documentation

#### 10.125.2.1 string `rpki.publication.sax_handler.name` = "msg" [static]

Definition at line 349 of file `publication.py`.

#### 10.125.2.2 `rpki.publication.sax_handler.pdu` = `msg` [static]

Reimplemented in [irbe\\_cli.publication\\_sax\\_handler](#).

Definition at line 348 of file `publication.py`.

#### 10.125.2.3 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 \(2481\)](#)

## 10.126 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.*

### 10.126.1 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.

### 10.126.2 Member Function Documentation

#### 10.126.2.1 `def rpki.resource_set.resource_bag.__eq__ ( self, other)`

Definition at line 600 of file resource\_set.py.

#### 10.126.2.2 `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.

#### 10.126.2.3 `def rpki.resource_set.resource_bag.__ne__ ( self, other)`

Definition at line 606 of file resource\_set.py.

#### 10.126.2.4 `def rpki.resource_set.resource_bag.__str__ ( self)`

Definition at line 629 of file resource\_set.py.

#### 10.126.2.5 `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.

#### 10.126.2.6 `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.

**10.126.2.7 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.

**10.126.2.8 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.

**10.126.2.9 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.

**10.126.2.10 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.

**10.126.3 Member Data Documentation****10.126.3.1 rpki::resource\_set.resource\_bag::asn**

Set of Autonomous System Number resources.

Definition at line 551 of file resource\_set.py.

### 10.126.3.2 rpki::resource\_set.resource\_bag::v4

Set of IPv4 resources.

Definition at line 552 of file resource\_set.py.

### 10.126.3.3 rpki::resource\_set.resource\_bag::v6

Set of IPv6 resources.

Definition at line 553 of file resource\_set.py.

### 10.126.3.4 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 \(2457\)](#)

## 10.127 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](#)

### 10.127.1 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.

### 10.127.2 Member Function Documentation

#### 10.127.2.1 def rpki.resource\_set.resource\_range.\_\_cmp\_\_ ( *self*, *other* )

Compare two resource\_range objects.

Definition at line 67 of file resource\_set.py.

#### 10.127.2.2 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.

### 10.127.3 Member Data Documentation

#### 10.127.3.1 rpki.resource\_set.resource\_range.max

Definition at line 65 of file resource\_set.py.

#### 10.127.3.2 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)



## 10.128 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).*

### 10.128.1 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.

### 10.128.2 Member Function Documentation

#### 10.128.2.1 `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.

#### 10.128.2.2 `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`.

### 10.128.3 Member Data Documentation

#### 10.128.3.1 `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`.

#### 10.128.3.2 `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 \(2457\)](#)

## 10.129 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](#)

### 10.129.1 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.

### 10.129.2 Member Function Documentation

#### 10.129.2.1 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.

#### 10.129.2.2 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.

#### 10.129.2.3 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.

### 10.129.2.4 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 \(2457\)](#)

## 10.130 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).*

### 10.130.1 Detailed Description

Range of IPv4 addresses.

Definition at line 170 of file resource\_set.py.

### 10.130.2 Member Data Documentation

#### 10.130.2.1 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 \(2457\)](#)

## 10.131 `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).*

### 10.131.1 Detailed Description

Range of IPv6 addresses.

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

### 10.131.2 Member Data Documentation

**10.131.2.1** `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 \(2457\)](#)

## 10.132 `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](#)

#### 10.132.1 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.

#### 10.132.2 Member Function Documentation

##### 10.132.2.1 def rpki.resource\_set.resource\_set.\_\_init\_\_ ( self, ini = None)

Initialize a resource\_set.

Definition at line 219 of file resource\_set.py.

##### 10.132.2.2 def rpki.resource\_set.resource\_set.\_\_str\_\_ ( self)

Convert a resource\_set to string format.

Definition at line 246 of file resource\_set.py.

### 10.132.2.3 `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`.

### 10.132.2.4 `def rpki.resource_set.resource_set.contains ( self, item)`

Set membership test for resource sets.

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

### 10.132.2.5 `def rpki.resource_set.resource_set.difference ( self, other)`

Set difference for resource sets.

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

### 10.132.2.6 `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`.

**10.132.2.7 def rpki.resource\_set.resource\_set.intersection ( *self*, *other* )**

Set intersection for resource sets.

Definition at line 313 of file resource\_set.py.

**10.132.2.8 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.

**10.132.2.9 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.

**10.132.2.10 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.

**10.132.2.11 def rpki.resource\_set.resource\_set.union ( *self*, *other* )**

Set union for resource sets.

Definition at line 288 of file resource\_set.py.



### 10.132.3 Member Data Documentation

#### 10.132.3.1 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)

### 10.133 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](#).*

#### 10.133.1 Detailed Description

Autonomous System Number resource set.

Definition at line 369 of file `resource_set.py`.

### 10.133.2 Member Function Documentation

#### 10.133.2.1 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.

#### 10.133.2.2 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.

#### 10.133.2.3 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.

### 10.133.3 Member Data Documentation

#### 10.133.3.1 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.

#### 10.133.3.2 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)

## 10.134 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.*

### 10.134.1 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.

### 10.134.2 Member Function Documentation

#### 10.134.2.1 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.

### 10.134.2.2 `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`.

### 10.134.2.3 `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`.

## 10.134.3 Member Data Documentation

### 10.134.3.1 `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 \(2457\)](#)

## 10.135 `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](#).*

### 10.135.1 Detailed Description

IPv4 address resource set.

Definition at line 469 of file resource\_set.py.

### 10.135.2 Member Data Documentation

#### 10.135.2.1 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.

#### 10.135.2.2 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 \(2457\)](#)

## 10.136 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](#).*

### 10.136.1 Detailed Description

IPv6 address resource set.

Definition at line 484 of file resource\_set.py.

### 10.136.2 Member Data Documentation

#### 10.136.2.1 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.

#### 10.136.2.2 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 \(2457\)](#)

## 10.137 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.*

### 10.137.1 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`.

### 10.137.2 Member Function Documentation

#### 10.137.2.1 `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`.

#### 10.137.2.2 `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`.

**10.137.2.3 def rpki.resource\_set.roa\_prefix.\_\_str\_\_ ( self)**

Convert a ROA prefix to string format.

Definition at line 694 of file resource\_set.py.

**10.137.2.4 def rpki.resource\_set.roa\_prefix.max ( self)**

Return highest address covered by prefix.

Definition at line 715 of file resource\_set.py.

**10.137.2.5 def rpki.resource\_set.roa\_prefix.min ( self)**

Return lowest address covered by prefix.

Definition at line 711 of file resource\_set.py.

**10.137.2.6 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.

**10.137.2.7 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.



### 10.137.3 Member Data Documentation

#### 10.137.3.1 rpki::resource\_set.roa\_prefix::address

Address portion of prefix.

Definition at line 677 of file resource\_set.py.

#### 10.137.3.2 rpki::resource\_set.roa\_prefix::max\_prefixlen

Maximum prefix length.

Definition at line 679 of file resource\_set.py.

#### 10.137.3.3 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 \(2457\)](#)

### 10.138 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](#).*

#### 10.138.1 Detailed Description

IPv4 ROA prefix.

Definition at line 730 of file resource\_set.py.

## 10.138.2 Member Data Documentation

**10.138.2.1** `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)

## 10.139 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](#).*

## 10.139.1 Detailed Description

IPv6 ROA prefix.

Definition at line 740 of file `resource_set.py`.

## 10.139.2 Member Data Documentation

**10.139.2.1** `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)

## 10.140 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](#)

#### 10.140.1 Detailed Description

Set of ROA prefixes, analogous to the `resource_set_ip` class.

Definition at line 750 of file `resource_set.py`.

#### 10.140.2 Member Function Documentation

##### 10.140.2.1 `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`.

##### 10.140.2.2 `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`.

**10.140.2.3** `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.

**10.140.2.4** `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.

**10.140.2.5** `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.

**10.140.2.6** `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 \(2457\)](#)

## 10.141 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.*

### 10.141.1 Detailed Description

Set of IPv4 ROA prefixes.

Definition at line 834 of file [resource\\_set.py](#).

### 10.141.2 Member Data Documentation

#### 10.141.2.1 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](#).

#### 10.141.2.2 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)

## 10.142 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.*

### 10.142.1 Detailed Description

Set of IPv6 ROA prefixes.

Definition at line 849 of file [resource\\_set.py](#).

### 10.142.2 Member Data Documentation

#### 10.142.2.1 [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](#).

#### 10.142.2.2 [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)

## 10.143 rpki.roa.ROAIPAddress Class Reference

Inherits [Sequence](#).

### Public Member Functions

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

### Public Attributes

- [address](#)
- [maxLength](#)

#### 10.143.1 Detailed Description

Definition at line 47 of file roa.py.

#### 10.143.2 Member Function Documentation

##### 10.143.2.1 `def rpki.roa.ROAIPAddress.__init__ ( self, optional = 0, default = "" )`

Definition at line 48 of file roa.py.

#### 10.143.3 Member Data Documentation

##### 10.143.3.1 `rpki.roa.ROAIPAddress.address`

Definition at line 49 of file roa.py.

##### 10.143.3.2 `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 \(2424\)](#)

## 10.144 rpki.roa.ROAIPAddresses Class Reference

Inherits [SequenceOf](#).

### Public Member Functions

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

#### 10.144.1 Detailed Description

Definition at line 54 of file roa.py.

#### 10.144.2 Member Function Documentation

- 10.144.2.1** `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 \(2424\)](#)

## 10.145 rpki.roa.ROAIPAddressFamilies Class Reference

Inherits [SequenceOf](#).

### Public Member Functions

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

#### 10.145.1 Detailed Description

Definition at line 65 of file roa.py.



### 10.145.2 Member Function Documentation

**10.145.2.1** `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 \(2424\)](#)

## 10.146 rpki.roa.ROAIPAddressFamily Class Reference

Inherits [Sequence](#).

### Public Member Functions

- `def __init__`

### Public Attributes

- [addresses](#)
- [addressFamily](#)

### 10.146.1 Detailed Description

Definition at line 58 of file roa.py.

### 10.146.2 Member Function Documentation

**10.146.2.1** `def rpki.roa.ROAIPAddressFamily.__init__ ( self, optional = 0, default = '' )`

Definition at line 59 of file roa.py.

### 10.146.3 Member Data Documentation

#### 10.146.3.1 rpki.roa.ROAIPAddressFamily.addresses

Definition at line 61 of file roa.py.

#### 10.146.3.2 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 \(2424\)](#)

## 10.147 rpki.roa.RouteOriginAttestation Class Reference

Inherits [Sequence](#).

### Public Member Functions

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

### Public Attributes

- [asID](#)
- [explicitVersion](#)
- [ipAddrBlocks](#)
- [version](#)

#### 10.147.1 Detailed Description

Definition at line 69 of file roa.py.

#### 10.147.2 Member Function Documentation

- 10.147.2.1** `def rpki.roa.RouteOriginAttestation.__init__ ( self, optional = 0, default = '' )`

Definition at line 70 of file roa.py.

### 10.147.3 Member Data Documentation

#### 10.147.3.1 rpki.roa.RouteOriginAttestation.asID

Definition at line 73 of file roa.py.

#### 10.147.3.2 rpki.roa.RouteOriginAttestation.explicitVersion

Definition at line 72 of file roa.py.

#### 10.147.3.3 rpki.roa.RouteOriginAttestation.ipAddrBlocks

Definition at line 74 of file roa.py.

#### 10.147.3.4 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 \(2424\)](#)

### 10.148 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](#)

#### 10.148.1 Detailed Description

Internal CA detail object.

Definition at line 445 of file `rpki_engine.py`.

### 10.148.2 Member Function Documentation

#### 10.148.2.1 `def rpki.rpki_engine.ca_detail_obj.activate (self, ca, cert, uri, callback, errback, predecessor = None)`

Activate this ca\_detail.

Definition at line 503 of file rpki\_engine.py.

#### 10.148.2.2 `def rpki.rpki_engine.ca_detail_obj.ca (self)`

Fetch CA object to which this ca\_detail links.

Definition at line 475 of file rpki\_engine.py.

#### 10.148.2.3 `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 479 of file rpki\_engine.py.

#### 10.148.2.4 `def rpki.rpki_engine.ca_detail_obj.create (cls, ca)`

Create a new ca\_detail object for a specified CA.

Definition at line 657 of file rpki\_engine.py.

#### 10.148.2.5 `def rpki.rpki_engine.ca_detail_obj.crl_uri (self, ca)`

Return publication URI for this ca\_detail's CRL.

Definition at line 491 of file rpki\_engine.py.

**10.148.2.6 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 495 of file rpki\_engine.py.

**10.148.2.7 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 536 of file rpki\_engine.py.

**10.148.2.8 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 748 of file rpki\_engine.py.

**10.148.2.9 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 782 of file rpki\_engine.py.

**10.148.2.10 def rpki.rpki\_engine.ca\_detail\_obj.generate\_manifest\_cert ( self, ca)**

Generate a new manifest certificate for this ca\_detail.

Definition at line 692 of file rpki\_engine.py.

**10.148.2.11** `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 704 of file rpki\_engine.py.

**10.148.2.12** `def rpki.rpki_engine.ca_detail_obj.issue_ee ( self, ca, resources, subject_key, sia = None)`

Issue a new EE certificate.

Definition at line 675 of file rpki\_engine.py.

**10.148.2.13** `def rpki.rpki_engine.ca_detail_obj.manifest_uri ( self, ca)`

Return publication URI for this ca\_detail's manifest.

Definition at line 499 of file rpki\_engine.py.

**10.148.2.14** `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 564 of file rpki\_engine.py.

#### 10.148.2.15 def rpki.rpki\_engine.ca\_detail\_obj.revoked\_certs ( self)

Fetch all revoked\_cert objects that link to this ca\_detail.

Definition at line 483 of file rpki\_engine.py.

#### 10.148.2.16 def rpki.rpki\_engine.ca\_detail\_obj.route\_origins ( self)

Fetch all route\_origin objects that link to this ca\_detail.

Definition at line 487 of file rpki\_engine.py.

#### 10.148.2.17 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 465 of file rpki\_engine.py.

#### 10.148.2.18 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 628 of file rpki\_engine.py.



### 10.148.3 Member Data Documentation

#### 10.148.3.1 rpki.rpki\_engine.ca\_detail\_obj.ca\_cert\_uri

Definition at line 509 of file rpki\_engine.py.

#### 10.148.3.2 rpki.rpki\_engine.ca\_detail\_obj.ca\_id

Definition at line 663 of file rpki\_engine.py.

#### 10.148.3.3 rpki.rpki\_engine.ca\_detail\_obj.gctx

Reimplemented from [rpki.sql.sql\\_persistent](#).

Definition at line 662 of file rpki\_engine.py.

#### 10.148.3.4 rpki.rpki\_engine.ca\_detail\_obj.latest\_ca\_cert

Definition at line 508 of file rpki\_engine.py.

#### 10.148.3.5 rpki.rpki\_engine.ca\_detail\_obj.latest\_crl

Definition at line 772 of file rpki\_engine.py.

#### 10.148.3.6 rpki.rpki\_engine.ca\_detail\_obj.latest\_manifest

Definition at line 806 of file rpki\_engine.py.

#### 10.148.3.7 rpki.rpki\_engine.ca\_detail\_obj.latest\_manifest\_cert

Definition at line 619 of file rpki\_engine.py.

### 10.148.3.8 rpki.rpki\_engine.ca\_detail\_obj.manifest\_private\_key\_id

Definition at line 617 of file rpki\_engine.py.

### 10.148.3.9 rpki.rpki\_engine.ca\_detail\_obj.manifest\_public\_key

Definition at line 618 of file rpki\_engine.py.

### 10.148.3.10 rpki.rpki\_engine.ca\_detail\_obj.nextUpdate

Definition at line 596 of file rpki\_engine.py.

### 10.148.3.11 rpki.rpki\_engine.ca\_detail\_obj.private\_key\_id

Definition at line 616 of file rpki\_engine.py.

### 10.148.3.12 rpki.rpki\_engine.ca\_detail\_obj.public\_key

Definition at line 667 of file rpki\_engine.py.

### 10.148.3.13 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 450 of file rpki\_engine.py.

### 10.148.3.14 rpki.rpki\_engine.ca\_detail\_obj.state

Definition at line 516 of file rpki\_engine.py.

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

- [rpki\\_engine.py \(2481\)](#)

## 10.149 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`

#### 10.149.1 Detailed Description

Internal CA object.

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

#### 10.149.2 Member Function Documentation

##### 10.149.2.1 `def rpki.rpki_engine.ca_obj.ca_details ( self )`

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

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

##### 10.149.2.2 `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 274 of file `rpki_engine.py`.

##### 10.149.2.3 `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 261 of file `rpki_engine.py`.

**10.149.2.4 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 332 of file rpki\_engine.py.

**10.149.2.5 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 356 of file rpki\_engine.py.

**10.149.2.6 def rpki.rpki\_engine.ca\_obj.fetch\_active ( self)**

Fetch the active ca\_detail for this CA, if any.

Definition at line 249 of file rpki\_engine.py.

**10.149.2.7 def rpki.rpki\_engine.ca\_obj.fetch\_deprecated ( self)**

Fetch deprecated ca\_details for this CA, if any.

Definition at line 253 of file rpki\_engine.py.

**10.149.2.8 def rpki.rpki\_engine.ca\_obj.fetch\_pending ( self)**

Fetch the pending ca\_details for this CA, if any.

Definition at line 245 of file rpki\_engine.py.

**10.149.2.9 def rpki.rpki\_engine.ca\_obj.fetch\_revoked ( *self* )**

Fetch revoked ca\_details for this CA, if any.

Definition at line 257 of file rpki\_engine.py.

**10.149.2.10 def rpki.rpki\_engine.ca\_obj.next\_crl\_number ( *self* )**

Allocate a CRL serial number.

Definition at line 400 of file rpki\_engine.py.

**10.149.2.11 def rpki.rpki\_engine.ca\_obj.next\_manifest\_number ( *self* )**

Allocate a manifest serial number.

Definition at line 392 of file rpki\_engine.py.

**10.149.2.12 def rpki.rpki\_engine.ca\_obj.next\_serial\_number ( *self* )**

Allocate a certificate serial number.

Definition at line 384 of file rpki\_engine.py.

**10.149.2.13 def rpki.rpki\_engine.ca\_obj.parent ( *self* )**

Fetch parent object to which this CA object links.

Definition at line 237 of file rpki\_engine.py.

**10.149.2.14 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 408 of file rpki\_engine.py.

**10.149.2.15 def rpki.rpki\_engine.ca\_obj.revoke ( self, cb, eb)**

Revoke deprecated ca\_detail objects associated with this ca.

Definition at line 433 of file rpki\_engine.py.

**10.149.3 Member Data Documentation****10.149.3.1 rpki.rpki\_engine.ca\_obj.gctx**

Reimplemented from [rpki.sql.sql\\_persistent](#).

Definition at line 339 of file rpki\_engine.py.

**10.149.3.2 int rpki.rpki\_engine.ca\_obj.last\_crl\_sn = 0 [static]**

Definition at line 233 of file rpki\_engine.py.

**10.149.3.3 int rpki.rpki\_engine.ca\_obj.last\_issued\_sn = 0 [static]**

Definition at line 234 of file rpki\_engine.py.

**10.149.3.4 int rpki.rpki\_engine.ca\_obj.last\_manifest\_sn = 0 [static]**

Definition at line 235 of file rpki\_engine.py.

### 10.149.3.5 rpki.rpki\_engine.ca\_obj.parent\_id

Definition at line 340 of file rpki\_engine.py.

### 10.149.3.6 rpki.rpki\_engine.ca\_obj.parent\_resource\_class

Definition at line 341 of file rpki\_engine.py.

### 10.149.3.7 rpki.rpki\_engine.ca\_obj.sia\_uri

Definition at line 285 of file rpki\_engine.py.

### 10.149.3.8 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 224 of file rpki\_engine.py.

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

- [rpki\\_engine.py \(2481\)](#)

## 10.150 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](#)

#### 10.150.1 Detailed Description

Certificate that has been issued to a child.

Definition at line 816 of file `rpki_engine.py`.

#### 10.150.2 Member Function Documentation

**10.150.2.1** `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 829 of file `rpki_engine.py`.

**10.150.2.2** `def rpki.rpki_engine.child_cert_obj.ca_detail ( self)`

Fetch `ca_detail` object to which this `child_cert` object links.

Definition at line 845 of file `rpki_engine.py`.

**10.150.2.3 def rpki.rpki\_engine.child\_cert\_obj.child ( self)**

Fetch child object to which this child\_cert object links.

Definition at line 841 of file rpki\_engine.py.

**10.150.2.4 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 951 of file rpki\_engine.py.

**10.150.2.5 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 878 of file rpki\_engine.py.

**10.150.2.6 def rpki.rpki\_engine.child\_cert\_obj.revoke ( self, callback, errback, withdraw = True)**

Revoke a child cert.

Definition at line 857 of file rpki\_engine.py.

**10.150.2.7 `def rpki.rpki_engine.child_cert_obj.uri ( self, ca )`**

Return the publication URI for this `child_cert`.

Definition at line 853 of file `rpki_engine.py`.

**10.150.2.8 `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 849 of file `rpki_engine.py`.

**10.150.3 Member Data Documentation****10.150.3.1 `rpki.rpki_engine.child_cert_obj.ca_detail_id`**

Definition at line 836 of file `rpki_engine.py`.

**10.150.3.2 `rpki.rpki_engine.child_cert_obj.cert`**

Definition at line 837 of file `rpki_engine.py`.

**10.150.3.3 `rpki.rpki_engine.child_cert_obj.child_id`**

Definition at line 835 of file `rpki_engine.py`.

**10.150.3.4 `rpki.rpki_engine.child_cert_obj.gctx`**

Reimplemented from [rpki.sql.sql\\_persistent](#).

Definition at line 834 of file `rpki_engine.py`.

### 10.150.3.5 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 821 of file rpki\_engine.py.

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

- [rpki\\_engine.py \(2481\)](#)

## 10.151 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](#)

### 10.151.1 Detailed Description

Tombstone for a revoked certificate.

Definition at line 983 of file rpki\_engine.py.

### 10.151.2 Member Function Documentation

**10.151.2.1** `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 996 of file rpki\_engine.py.

**10.151.2.2** `def rpki.rpki_engine.revoked_cert_obj.ca_detail ( self)`

Fetch ca\_detail object to which this revoked\_cert\_obj links.

Definition at line 1007 of file rpki\_engine.py.

**10.151.2.3** `def rpki.rpki_engine.revoked_cert_obj.revoke ( cls, cert, ca_detail)`

Revoke a certificate.

Definition at line 1012 of file rpki\_engine.py.

### 10.151.3 Member Data Documentation

**10.151.3.1** `rpki.rpki_engine.revoked_cert_obj.ca_detail_id`

Definition at line 1003 of file rpki\_engine.py.

### 10.151.3.2 `rpki.rpki_engine.revoked_cert_obj.expires`

Definition at line 1002 of file `rpki_engine.py`.

### 10.151.3.3 `rpki.rpki_engine.revoked_cert_obj.gctx`

Reimplemented from [rpki.sql.sql\\_persistent](#).

Definition at line 999 of file `rpki_engine.py`.

### 10.151.3.4 `rpki.rpki_engine.revoked_cert_obj.revoked`

Definition at line 1001 of file `rpki_engine.py`.

### 10.151.3.5 `rpki.rpki_engine.revoked_cert_obj.serial`

Definition at line 1000 of file `rpki_engine.py`.

### 10.151.3.6 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 988 of file `rpki_engine.py`.

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

- [rpki\\_engine.py \(2481\)](#)

## 10.152 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 [left\\_right\\_handler](#)
- def [up\\_down\\_handler](#)

### Public Attributes

- [bpci\\_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)

### 10.152.1 Detailed Description

A container for various global rpkid parameters.

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

### 10.152.2 Member Function Documentation

#### 10.152.2.1 `def rpki.rpki_engine.rpkid_context.__init__ ( self, cfg )`

Definition at line 44 of file `rpki_engine.py`.

#### 10.152.2.2 `def rpki.rpki_engine.rpkid_context.build_https_ta_cache ( self )`

Build dynamic TLS trust anchors.

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

#### 10.152.2.3 `def rpki.rpki_engine.rpkid_context.clear_https_ta_cache ( self )`

Clear dynamic TLS trust anchors.

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

#### 10.152.2.4 `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 150 of file `rpki_engine.py`.

#### 10.152.2.5 `def rpki.rpki_engine.rpkid_context.irdb_query ( self, self_id, child_id, callback, errback )`

Perform an IRDB callback query.

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



### 10.152.2.6 `def rpki.rpki_engine.rpkid_context.left_right_handler ( self, query, path, cb)`

Process one left-right PDU.

Definition at line 96 of file rpki\_engine.py.

### 10.152.2.7 `def rpki.rpki_engine.rpkid_context.up_down_handler ( self, query, path, cb)`

Process one up-down PDU.

Definition at line 122 of file rpki\_engine.py.

## 10.152.3 Member Data Documentation

### 10.152.3.1 `rpki.rpki_engine.rpkid_context.bpki_ta`

Definition at line 48 of file rpki\_engine.py.

### 10.152.3.2 `rpki.rpki_engine.rpkid_context.https_server_host`

Definition at line 56 of file rpki\_engine.py.

### 10.152.3.3 `rpki.rpki_engine.rpkid_context.https_server_port`

Definition at line 57 of file rpki\_engine.py.

### 10.152.3.4 `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 188 of file rpki\_engine.py.

**10.152.3.5 rpki.rpki\_engine.rpkid\_context.irbe\_cert**

Definition at line 50 of file rpki\_engine.py.

**10.152.3.6 rpki.rpki\_engine.rpkid\_context.irdb\_cert**

Definition at line 49 of file rpki\_engine.py.

**10.152.3.7 rpki.rpki\_engine.rpkid\_context.irdb\_url**

Definition at line 54 of file rpki\_engine.py.

**10.152.3.8 rpki.rpki\_engine.rpkid\_context.publication\_kludge\_base**

Definition at line 59 of file rpki\_engine.py.

**10.152.3.9 rpki.rpki\_engine.rpkid\_context.rpkid\_cert**

Definition at line 51 of file rpki\_engine.py.

**10.152.3.10 rpki.rpki\_engine.rpkid\_context.rpkid\_key**

Definition at line 52 of file rpki\_engine.py.

**10.152.3.11 rpki.rpki\_engine.rpkid\_context.sql**

Definition at line 46 of file rpki\_engine.py.

```
10.152.3.12 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 120 of file rpki\_engine.py.

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

- [rpki\\_engine.py \(2481\)](#)

## 10.153 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

#### 10.153.1 Detailed Description

SQL session layer.

Definition at line 38 of file sql.py.

#### 10.153.2 Member Function Documentation

##### 10.153.2.1 `def rpki.sql.session.__init__ ( self, cfg)`

Definition at line 45 of file sql.py.

##### 10.153.2.2 `def rpki.sql.session._wrap_execute ( self, func, query, args)` [private]

Definition at line 75 of file sql.py.

##### 10.153.2.3 `def rpki.sql.session.assert_pristine ( self)`

Assert that there are no dirty objects in the cache.

Definition at line 99 of file sql.py.

##### 10.153.2.4 `def rpki.sql.session.cache_clear ( self)`

Clear the object cache.

Definition at line 95 of file sql.py.

**10.153.2.5 def rpki.sql.session.close ( *self* )**

Definition at line 64 of file sql.py.

**10.153.2.6 def rpki.sql.session.connect ( *self* )**

Definition at line 60 of file sql.py.

**10.153.2.7 def rpki.sql.session.execute ( *self*, *query*, *args* = None )**

Definition at line 83 of file sql.py.

**10.153.2.8 def rpki.sql.session.executemany ( *self*, *query*, *args* )**

Definition at line 86 of file sql.py.

**10.153.2.9 def rpki.sql.session.fetchall ( *self* )**

Definition at line 89 of file sql.py.

**10.153.2.10 def rpki.sql.session.lastrowid ( *self* )**

Definition at line 92 of file sql.py.

**10.153.2.11 def rpki.sql.session.ping ( *self* )**

Definition at line 72 of file sql.py.

**10.153.2.12 def rpki.sql.session.sweep ( *self* )**

Write any dirty objects out to SQL.

Definition at line 103 of file sql.py.

### 10.153.3 Member Data Documentation

#### 10.153.3.1 `rpki.sql.session._exceptions_enabled = False` [static, private]

Definition at line 43 of file sql.py.

#### 10.153.3.2 `rpki.sql.session.cache`

Definition at line 55 of file sql.py.

#### 10.153.3.3 `rpki.sql.session.cur`

Definition at line 62 of file sql.py.

#### 10.153.3.4 `rpki.sql.session.database`

Definition at line 52 of file sql.py.

#### 10.153.3.5 `rpki.sql.session.db`

Definition at line 61 of file sql.py.

#### 10.153.3.6 `rpki.sql.session.dirty`

Definition at line 56 of file sql.py.

### 10.153.3.7 rpki.sql.session.password

Definition at line 53 of file sql.py.

### 10.153.3.8 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 \(2452\)](#)

## 10.154 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](#) = True  
*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.*

#### 10.154.1 Detailed Description

Mixin for persistent class that needs to be stored in SQL.

Definition at line 139 of file sql.py.

#### 10.154.2 Member Function Documentation

##### 10.154.2.1 `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 307 of file sql.py.

##### 10.154.2.2 `def rpki.sql.sql_persistent.sql_delete ( self)`

Delete this object from SQL.

Definition at line 280 of file sql.py.



**10.154.2.3 def rpki.sql.sql\_persistent.sql\_delete\_hook ( self)**

Customization hook.

Reimplemented in [rpki.left\\_right.route\\_origin\\_elt](#).

Definition at line 333 of file sql.py.

**10.154.2.4 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 294 of file sql.py.

**10.154.2.5 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 160 of file sql.py.

**10.154.2.6 def rpki.sql.sql\_persistent.sql\_fetch\_all ( cls, gctx)**

Fetch all objects of this type from SQL.

Definition at line 198 of file sql.py.

**10.154.2.7** `def rpki.sql.sql_persistent.sql_fetch_hook ( self)`

Customization hook.

Reimplemented in [rpki.left\\_right.route\\_origin\\_elt](#).

Definition at line 320 of file sql.py.

**10.154.2.8** `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 203 of file sql.py.

**10.154.2.9** `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 183 of file sql.py.

**10.154.2.10** `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 230 of file sql.py.

**10.154.2.11** `def rpki.sql.sql_persistent.sql_insert_hook ( self)`

Customization hook.

Reimplemented in [rpki.left\\_right.route\\_origin\\_elt](#).

Definition at line 324 of file sql.py.

**10.154.2.12 def rpki.sql.sql\_persistent.sql\_is\_dirty ( *self* )**

Query whether this object needs to be written back to SQL.

Definition at line 250 of file sql.py.

**10.154.2.13 def rpki.sql.sql\_persistent.sql\_mark\_clean ( *self* )**

Mark this object as not needing to be written back to SQL.

Definition at line 246 of file sql.py.

**10.154.2.14 def rpki.sql.sql\_persistent.sql\_mark\_deleted ( *self* )**

Mark this object as needing to be deleted in SQL.

Definition at line 254 of file sql.py.

**10.154.2.15 def rpki.sql.sql\_persistent.sql\_mark\_dirty ( *self* )**

Mark this object as needing to be written back to SQL.

Definition at line 242 of file sql.py.

**10.154.2.16 def rpki.sql.sql\_persistent.sql\_store ( *self* )**

Store this object to SQL.

Definition at line 258 of file sql.py.

**10.154.2.17** `def rpki.sql.sql_persistent.sql_update_hook ( self )`

Customization hook.

Definition at line 328 of file sql.py.

**10.154.3 Member Data Documentation****10.154.3.1** `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 235 of file sql.py.

**10.154.3.2** `rpki::sql.sql_persistent::sql_debug = True` `[static]`

Enable logging of SQL actions.

Definition at line 157 of file sql.py.

**10.154.3.3** `rpki::sql.sql_persistent::sql_deleted = False` `[static]`

Whether our cached copy of this [object](#) has been deleted.

Definition at line 152 of file sql.py.

**10.154.3.4** `rpki::sql.sql_persistent::sql_in_db = False` `[static]`

Whether this [object](#) is already in SQL or not.

Definition at line 147 of file sql.py.

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

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

## 10.155 rpki.sql.template Class Reference

Inherits [object](#).

### Public Member Functions

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

### Public Attributes

- [columns](#)
- [delete](#)
- [index](#)
- [insert](#)
- [map](#)
- [select](#)
- [table](#)
- [update](#)

### 10.155.1 Detailed Description

SQL template generator.

Definition at line 115 of file sql.py.

### 10.155.2 Member Function Documentation

#### 10.155.2.1 `def rpki.sql.template.__init__ ( self, table_name, index_column, data_columns)`

Build a SQL template.

Definition at line 120 of file sql.py.

### 10.155.3 Member Data Documentation

#### 10.155.3.1 `rpki.sql.template.columns`

Definition at line 127 of file sql.py.

### 10.155.3.2 rpki.sql.template.delete

Definition at line 137 of file sql.py.

### 10.155.3.3 rpki.sql.template.index

Definition at line 126 of file sql.py.

### 10.155.3.4 rpki.sql.template.insert

Definition at line 130 of file sql.py.

### 10.155.3.5 rpki.sql.template.map

Definition at line 128 of file sql.py.

### 10.155.3.6 rpki.sql.template.select

Definition at line 129 of file sql.py.

### 10.155.3.7 rpki.sql.template.table

Definition at line 125 of file sql.py.

### 10.155.3.8 rpki.sql.template.update

Definition at line 133 of file sql.py.

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

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

## 10.156 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.*

### 10.156.1 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`.

### 10.156.2 Member Function Documentation

#### 10.156.2.1 def `rpki.sundial.datetime.__add__(self, other)`

Force correct class for timedelta results.

Definition at line 126 of file sundial.py.

#### 10.156.2.2 def rpki.sundial.datetime.\_\_str\_\_ ( *self* )

Definition at line 115 of file sundial.py.

#### 10.156.2.3 def rpki.sundial.datetime.\_\_sub\_\_ ( *self*, *other* )

Force correct class for timedelta results.

Definition at line 136 of file sundial.py.

#### 10.156.2.4 def rpki.sundial.datetime.earlier ( *self*, *other* )

Return the earlier of two timestamps.

Definition at line 170 of file sundial.py.

#### 10.156.2.5 def rpki.sundial.datetime.from\_sql ( *cls*, *x* )

Convert from SQL storage format.

Definition at line 147 of file sundial.py.

#### 10.156.2.6 def rpki.sundial.datetime.fromASN1tuple ( *cls*, *x* )

Convert from ASN.1 tuple representation.

Definition at line 77 of file sundial.py.



**10.156.2.7 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.

**10.156.2.8 def rpki.sundial.datetime.fromGeneralizedTime ( *cls*, *x* )**

Convert from ASN.1 GeneralizedTime.

Definition at line 68 of file sundial.py.

**10.156.2.9 def rpki.sundial.datetime.fromUTCTime ( *cls*, *x* )**

Convert from ASN.1 UTCTime.

Definition at line 59 of file sundial.py.

**10.156.2.10 def rpki.sundial.datetime.fromXMLtime ( *cls*, *x* )**

Convert from XML time representation.

Definition at line 102 of file sundial.py.

**10.156.2.11 def rpki.sundial.datetime.later ( *self*, *other* )**

Return the later of two timestamps.

Definition at line 166 of file sundial.py.

**10.156.2.12 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.

**10.156.2.13 def rpki.sundial.datetime.toASN1tuple ( self)**

Convert to ASN.1 tuple representation.

Definition at line 92 of file sundial.py.

**10.156.2.14 def rpki.sundial.datetime.toGeneralizedTime ( self)**

Convert to ASN.1 GeneralizedTime.

Definition at line 72 of file sundial.py.

**10.156.2.15 def rpki.sundial.datetime.totimestamp ( self)**

Convert to seconds from epoch (like time.time()). Conversion method is a bit silly, but avoids time module timezone whackiness.

Definition at line 51 of file sundial.py.

**10.156.2.16 def rpki.sundial.datetime.toUTCTime ( self)**

Convert to ASN.1 UTCTime.

Definition at line 63 of file sundial.py.

### 10.156.2.17 def rpki.sundial.datetime.toXMLtime ( self)

Convert to XML time representation.

Definition at line 111 of file sundial.py.

### 10.156.3 Member Data Documentation

#### 10.156.3.1 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 \(2452\)](#)

## 10.157 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.*

### 10.157.1 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.

## 10.157.2 Member Function Documentation

### 10.157.2.1 def rpki.sundial.timedelta.convert\_to\_seconds ( *self* )

Convert a timedelta interval to seconds.

Definition at line 216 of file sundial.py.

### 10.157.2.2 def rpki.sundial.timedelta.fromtimedelta ( *cls*, *x* )

Convert a datetime.timedelta object into this subclass.

Definition at line 221 of file sundial.py.

### 10.157.2.3 def rpki.sundial.timedelta.parse ( *cls*, *arg* )

Parse text into a timedelta object.

Definition at line 200 of file sundial.py.

## 10.157.3 Member Data Documentation

### 10.157.3.1 rpki::sundial.timedelta::regexp [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 \(2452\)](#)

## 10.158 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](#)

### 10.158.1 Detailed Description

Generic PDU object.

Virtual class, just provides some default methods.

Definition at line 43 of file `up_down.py`.

## 10.158.2 Member Function Documentation

### 10.158.2.1 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.

### 10.158.2.2 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.

### 10.158.2.3 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.

### 10.158.2.4 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.

### 10.158.2.5 `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`.

### 10.158.2.6 `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 \(2481\)](#)

## 10.159 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](#)

### 10.159.1 Detailed Description

Up-Down protocol representation of an issued certificate.

Definition at line 128 of file up\_down.py.

### 10.159.2 Member Function Documentation

#### 10.159.2.1 `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.

#### 10.159.2.2 `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.

#### 10.159.2.3 `def rpki.up_down.certificate_elt.toXML ( self)`

Generate a <certificate/> element.

Definition at line 151 of file up\_down.py.



### 10.159.3 Member Data Documentation

#### 10.159.3.1 rpki.up\_down.certificate\_elt.cert

Definition at line 148 of file up\_down.py.

#### 10.159.3.2 rpki.up\_down.certificate\_elt.cert\_url

Definition at line 138 of file up\_down.py.

#### 10.159.3.3 rpki.up\_down.certificate\_elt.req\_resource\_set\_as

Definition at line 139 of file up\_down.py.

#### 10.159.3.4 rpki.up\_down.certificate\_elt.req\_resource\_set\_ipv4

Definition at line 140 of file up\_down.py.

#### 10.159.3.5 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 \(2481\)](#)

### 10.160 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

### 10.160.1 Detailed Description

Up-Down protocol representation of a resource class.

Definition at line 160 of file up\_down.py.

### 10.160.2 Member Function Documentation

#### 10.160.2.1 def rpki.up\_down.class\_elt.\_\_init\_\_ ( self)

Initialize class\_elt.

Definition at line 167 of file up\_down.py.

#### 10.160.2.2 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.

#### 10.160.2.3 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.

#### 10.160.2.4 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.

#### 10.160.2.5 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.

#### 10.160.2.6 def rpki.up\_down.class\_elt.toXML ( self)

Generate a <class/> element.

Definition at line 201 of file up\_down.py.

### 10.160.3 Member Data Documentation

#### 10.160.3.1 rpki.up\_down.class\_elt.cert\_url

Definition at line 184 of file up\_down.py.

**10.160.3.2 rpki.up\_down.class\_elt.certs**

Definition at line 170 of file up\_down.py.

**10.160.3.3 rpki.up\_down.class\_elt.class\_name**

Definition at line 183 of file up\_down.py.

**10.160.3.4 rpki.up\_down.class\_elt.issuer = None** [static]

Definition at line 165 of file up\_down.py.

**10.160.3.5 rpki.up\_down.class\_elt.resource\_set\_as**

Definition at line 186 of file up\_down.py.

**10.160.3.6 rpki.up\_down.class\_elt.resource\_set\_ipv4**

Definition at line 187 of file up\_down.py.

**10.160.3.7 rpki.up\_down.class\_elt.resource\_set\_ipv6**

Definition at line 188 of file up\_down.py.

**10.160.3.8 rpki.up\_down.class\_elt.resource\_set\_notafter**

Definition at line 189 of file up\_down.py.

### 10.160.3.9 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 \(2481\)](#)

## 10.161 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](#)

### 10.161.1 Detailed Description

Syntax for Up-Down protocol "list\_response" and "issue\_response" PDUs.

Definition at line 279 of file up\_down.py.

### 10.161.2 Member Function Documentation

#### 10.161.2.1 `def rpki.up_down.class_response_syntax.__init__ ( self)`

Initialize class\_response\_syntax.

Definition at line 284 of file up\_down.py.

### 10.161.2.2 `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.

### 10.161.2.3 `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.

## 10.161.3 Member Data Documentation

### 10.161.3.1 `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 \(2481\)](#)

## 10.162 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](#)

### 10.162.1 Detailed Description

Class to hold a CMS-signed up-down PDU.

Definition at line 670 of file up\_down.py.

### 10.162.2 Member Data Documentation

#### 10.162.2.1 string rpki.up\_down.cms\_msg.encoding = "UTF-8" [static]

Definition at line 675 of file up\_down.py.

#### 10.162.2.2 rpki.up\_down.cms\_msg.saxify = sax\_handler.saxify [static]

Reimplemented in [rootd.cms\\_msg](#).

Definition at line 677 of file up\_down.py.

#### 10.162.2.3 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](#) (2481)

## 10.163 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](#)

#### 10.163.1 Detailed Description

Up-Down protocol "error\_response" PDU.

Definition at line 497 of file up\_down.py.

#### 10.163.2 Member Function Documentation

##### 10.163.2.1 `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.

##### 10.163.2.2 `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.

##### 10.163.2.3 `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.

#### 10.163.2.4 def rpki.up\_down.error\_response\_pdu.toXML ( self)

Generate payload of "error\_response" PDU.

Definition at line 541 of file up\_down.py.

### 10.163.3 Member Data Documentation

#### 10.163.3.1 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.

#### 10.163.3.2 rpki.up\_down.error\_response\_pdu.description

Definition at line 523 of file up\_down.py.

#### 10.163.3.3 dictionary rpki.up\_down.error\_response\_pdu.exceptions [static]

**Initial value:**

```
{  
    rpki.exceptions.NoActiveCA : 1202 }
```

Definition at line 513 of file up\_down.py.

#### 10.163.3.4 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 \(2481\)](#)

### 10.164 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](#)

#### 10.164.1 Detailed Description

Up-Down protocol "issue" PDU.

Definition at line 309 of file up\_down.py.

## 10.164.2 Member Function Documentation

### 10.164.2.1 `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.

### 10.164.2.2 `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.

### 10.164.2.3 `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.

### 10.164.2.4 `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.

**10.164.2.5 def rpki.up\_down.issue\_pdu.toXML ( *self* )**

Generate payload of "issue" PDU.

Definition at line 332 of file up\_down.py.

**10.164.3 Member Data Documentation****10.164.3.1 rpki.up\_down.issue\_pdu.class\_name**

Definition at line 319 of file up\_down.py.

**10.164.3.2 rpki.up\_down.issue\_pdu.pkcs10**

Definition at line 329 of file up\_down.py.

**10.164.3.3 rpki.up\_down.issue\_pdu.req\_resource\_set\_as**

Definition at line 320 of file up\_down.py.

**10.164.3.4 rpki.up\_down.issue\_pdu.req\_resource\_set\_ipv4**

Definition at line 321 of file up\_down.py.

**10.164.3.5 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 \(2481\)](#)

## 10.165 rpki.up\_down.issue\_response\_pdu Class Reference

Inherits [rpki::up\\_down::class\\_response\\_syntax](#).

### Public Member Functions

- def [check\\_response](#)

### 10.165.1 Detailed Description

Up-Down protocol "issue\_response" PDU.

Definition at line 421 of file up\_down.py.

### 10.165.2 Member Function Documentation

#### 10.165.2.1 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](#) (2481)

## 10.166 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](#)

### 10.166.1 Detailed Description

Up-Down protocol "list" PDU.

Definition at line 231 of file up\_down.py.

### 10.166.2 Member Function Documentation

#### 10.166.2.1 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.

#### 10.166.2.2 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.

#### 10.166.2.3 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](#) (2481)

### 10.167 rpki.up\_down.list\_response\_pdu Class Reference

Inherits [rpki::up\\_down::class\\_response\\_syntax](#).

### 10.167.1 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 \(2481\)](#)

## 10.168 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

### 10.168.1 Detailed Description

Up-Down protocol message wrapper PDU.

Definition at line 563 of file up\_down.py.

## 10.168.2 Member Function Documentation

### 10.168.2.1 def rpki.up\_down.message\_pdu.\_\_str\_\_ ( *self* )

Convert a message PDU to a string.

Definition at line 605 of file up\_down.py.

### 10.168.2.2 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.

### 10.168.2.3 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.

### 10.168.2.4 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.

### 10.168.2.5 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.

#### 10.168.2.6 def rpki.up\_down.message\_pdu.toXML ( self)

Generate payload of message PDU.

Definition at line 581 of file up\_down.py.

### 10.168.3 Member Data Documentation

#### 10.168.3.1 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.

#### 10.168.3.2 rpki.up\_down.message\_pdu.payload

Definition at line 602 of file up\_down.py.

### 10.168.3.3 rpki.up\_down.message\_pdu.recipient

Definition at line 600 of file up\_down.py.

### 10.168.3.4 rpki.up\_down.message\_pdu.sender

Definition at line 599 of file up\_down.py.

### 10.168.3.5 rpki.up\_down.message\_pdu.type

Definition at line 601 of file up\_down.py.

### 10.168.3.6 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.

### 10.168.3.7 rpki.up\_down.message\_pdu.version

Definition at line 598 of file up\_down.py.

### 10.168.3.8 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 \(2481\)](#)

## 10.169 rpki.up\_down.multi\_uri Class Reference

Inherits list.

## Public Member Functions

- [def \\_\\_init\\_\\_](#)
- [def \\_\\_str\\_\\_](#)
- [def rsync](#)

### 10.169.1 Detailed Description

Container for a set of URIs.

Definition at line 95 of file up\_down.py.

### 10.169.2 Member Function Documentation

#### 10.169.2.1 `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.

#### 10.169.2.2 `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.

#### 10.169.2.3 `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 \(2481\)](#)

## 10.170 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](#)

#### 10.170.1 Detailed Description

Up-Down protocol "revoke" PDU.

Definition at line 448 of file up\_down.py.

#### 10.170.2 Member Function Documentation

##### 10.170.2.1 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.

##### 10.170.2.2 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.

### 10.170.2.3 `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`.

## 10.170.3 Member Data Documentation

### 10.170.3.1 `rpki.up_down.revoke_pdu.class_name`

Reimplemented from [rpki.up\\_down.revoke\\_syntax](#).

Definition at line 486 of file `up_down.py`.

### 10.170.3.2 `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 \(2481\)](#)

## 10.171 `rpki.up_down.revoke_response_pdu` Class Reference

Inherits [rpki::up\\_down::revoke\\_syntax](#).

### 10.171.1 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 \(2481\)](#)

## 10.172 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](#)

#### 10.172.1 Detailed Description

Syntax for Up-Down protocol "revoke" and "revoke\_response" PDUs.

Definition at line 434 of file up\_down.py.

#### 10.172.2 Member Function Documentation

##### 10.172.2.1 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.

##### 10.172.2.2 def rpki.up\_down.revoke\_syntax.toXML (*self*)

Generate payload of "revoke" PDU.

Definition at line 444 of file up\_down.py.

### 10.172.3 Member Data Documentation

#### 10.172.3.1 rpki.up\_down.revoke\_syntax.class\_name

Reimplemented in [rpki.up\\_down.revoke\\_pdu](#).

Definition at line 441 of file up\_down.py.

#### 10.172.3.2 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](#) (2481)

## 10.173 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"

### 10.173.1 Detailed Description

SAX handler for Up-Down protocol.

Definition at line 661 of file up\_down.py.

### 10.173.2 Member Data Documentation

#### 10.173.2.1 string rpki.up\_down.sax\_handler.name = "message" [static]

Definition at line 667 of file up\_down.py.

**10.173.2.2** `rpki.up_down.sax_handler.pdu = message_pdu` `[static]`

Reimplemented in [rootd.sax\\_handler](#).

Definition at line 666 of file up\_down.py.

**10.173.2.3** `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](#) (2481)

## 10.174 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.*

#### 10.174.1 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 691 of file x509.py.

#### 10.174.2 Member Function Documentation

##### 10.174.2.1 `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 842 of file `x509.py`.

#### 10.174.2.2 `def rpki.x509.CMS_object.get_content ( self)`

Get the inner content of this `CMS_object`.

Definition at line 753 of file `x509.py`.

#### 10.174.2.3 `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 732 of file `x509.py`.

#### 10.174.2.4 `def rpki.x509.CMS_object.get_POW ( self)`

Get the POW value of this `CMS_object`.

Definition at line 744 of file `x509.py`.

#### 10.174.2.5 `def rpki.x509.CMS_object.set_content ( self, content)`

Set the (inner) content of this `CMS_object`, clearing the wrapper.

Definition at line 760 of file `x509.py`.

**10.174.2.6** `def rpki.x509.CMS_object.sign ( self, keypair, certs, crls = None, no_certs = False)`

Sign and wrap inner content.

Definition at line 870 of file x509.py.

**10.174.2.7** `def rpki.x509.CMS_object.verify ( self, ta)`

Verify CMS wrapper and store inner content.

Definition at line 767 of file x509.py.

### 10.174.3 Member Data Documentation

#### 10.174.3.1 rpki.x509.CMS\_object.content

Reimplemented in [rpki.x509.DER\\_CMS\\_object](#), and [rpki.x509.XML\\_CMS\\_object](#).

Definition at line 765 of file x509.py.

**10.174.3.2** `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 717 of file x509.py.

#### 10.174.3.3 rpki.x509.CMS\_object.DER

DER value of this [object](#).

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 740 of file x509.py.

**10.174.3.4** `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 712 of file x509.py.

**10.174.3.5** `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 706 of file x509.py.

**10.174.3.6** `tuple rpki.x509.CMS_object.formats = ("DER", "POW")`  
[static]

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 704 of file x509.py.

**10.174.3.7** `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 705 of file x509.py.

**10.174.3.8** `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 707 of file x509.py.

#### 10.174.3.9 **rpki.x509.CMS\_object.POW**

Definition at line 750 of file x509.py.

#### 10.174.3.10 **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 730 of file x509.py.

#### 10.174.3.11 **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 724 of file x509.py.

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

- [x509.py \(2481\)](#)

### 10.175 **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](#).*

#### 10.175.1 Detailed Description

Class to hold a Certificate Revocation List.

Definition at line 1070 of file x509.py.

#### 10.175.2 Member Function Documentation

**10.175.2.1** `def rpki.x509.CRL.generate ( cls, keypair, issuer, serial, thisUpdate, nextUpdate, revokedCertificates, version = 1, digestType = "sha256WithRSAEncryption")`

Generate a new CRL.

Definition at line 1126 of file x509.py.

**10.175.2.2** `def rpki.x509.CRL.get_DER ( self)`

Get the DER value of this CRL.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 1078 of file x509.py.

**10.175.2.3 def rpki.x509.CRL.get\_POW ( self)**

Get the POW value of this CRL.

Definition at line 1093 of file x509.py.

**10.175.2.4 def rpki.x509.CRL.get\_POWpkix ( self)**

Get the POW.pkix value of this CRL.

Definition at line 1102 of file x509.py.

**10.175.2.5 def rpki.x509.CRL.getIssuer ( self)**

Get issuer value of this CRL.

Definition at line 1121 of file x509.py.

**10.175.2.6 def rpki.x509.CRL.getNextUpdate ( self)**

Get nextUpdate value from this CRL.

Definition at line 1117 of file x509.py.

**10.175.2.7 def rpki.x509.CRL.getThisUpdate ( self)**

Get thisUpdate value from this CRL.

Definition at line 1113 of file x509.py.

### 10.175.3 Member Data Documentation

#### 10.175.3.1 rpki.x509.CRL.DER

DER value of this [object](#).

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 1086 of file x509.py.

```
10.175.3.2 tuple rpki.x509.CRL.formats = ("DER", "POW", "POWpkix")  
[static]
```

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 1075 of file x509.py.

```
10.175.3.3 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 1076 of file x509.py.

#### 10.175.3.4 rpki.x509.CRL.POW

Definition at line 1099 of file x509.py.

#### 10.175.3.5 rpki.x509.CRL.POWpkix

Definition at line 1110 of file x509.py.

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

- [x509.py \(2481\)](#)



## 10.176 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](#)

#### 10.176.1 Detailed Description

Class to hold CMS objects with DER-based content.

Definition at line 906 of file x509.py.

#### 10.176.2 Member Function Documentation

##### 10.176.2.1 def rpki.x509.DER\_CMS\_object.decode ( self, der)

Decode DER and set inner content.

Definition at line 915 of file x509.py.

##### 10.176.2.2 def rpki.x509.DER\_CMS\_object.encode ( self)

Encode inner content for signing.

Definition at line 911 of file x509.py.

### 10.176.3 Member Data Documentation

#### 10.176.3.1 rpki.x509.DER\_CMS\_object.content

Reimplemented from [rpki.x509.CMS\\_object](#).

Definition at line 921 of file x509.py.

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

- [x509.py \(2481\)](#)

### 10.177 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](#).*

### 10.177.1 Detailed Description

Virtual class to hold a generic DER object.

Definition at line 104 of file x509.py.

### 10.177.2 Member Function Documentation

#### 10.177.2.1 def rpki.x509.DER\_object.\_\_cmp\_\_( self, other)

Compare two DER-encoded objects.

Definition at line 199 of file x509.py.

#### 10.177.2.2 def rpki.x509.DER\_object.\_\_init\_\_( self, kw)

Initialize a DER\_object.

Definition at line 137 of file x509.py.

**10.177.2.3 def rpki.x509.DER\_object.clear ( self)**

Make this object empty.

Definition at line 130 of file x509.py.

**10.177.2.4 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.

**10.177.2.5 def rpki.x509.DER\_object.empty ( self)**

Test whether this object is empty.

Definition at line 121 of file x509.py.

**10.177.2.6 def rpki.x509.DER\_object.from\_sql ( cls, x)**

Convert from SQL storage format.

Definition at line 290 of file x509.py.

**10.177.2.7 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.

**10.177.2.8 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.

**10.177.2.9 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.

**10.177.2.10 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.

**10.177.2.11 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.

**10.177.2.12 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.

**10.177.2.13 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.

**10.177.2.14 def rpki.x509.DER\_object.get\_PEM ( self)**

Get the PEM representation of this object.

Definition at line 195 of file x509.py.

**10.177.2.15 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.

**10.177.2.16 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.

**10.177.2.17 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.

**10.177.2.18 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.

**10.177.2.19 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.

**10.177.2.20 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.

**10.177.2.21 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.

#### 10.177.2.22 def rpki.x509.DER\_object.to\_sql ( self)

Convert to SQL storage format.

Definition at line 294 of file x509.py.

### 10.177.3 Member Data Documentation

#### 10.177.3.1 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.

#### 10.177.3.2 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.

#### 10.177.3.3 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.

#### 10.177.3.4 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 \(2481\)](#)

## 10.178 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](#)

### 10.178.1 Detailed Description

Convert between DER and PEM encodings for various kinds of ASN.1 data.

Definition at line 61 of file x509.py.

### 10.178.2 Member Function Documentation

#### 10.178.2.1 `def rpki.x509.PEM_converter.__init__ ( self, kind)`

Initialize PEM\_converter.

Definition at line 66 of file x509.py.

**10.178.2.2 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.

**10.178.2.3 def rpki.x509.PEM\_converter.to\_DER ( self, pem)**

Convert from PEM to DER.

Definition at line 80 of file x509.py.

**10.178.2.4 def rpki.x509.PEM\_converter.to\_PEM ( self, der)**

Convert from DER to PEM.

Definition at line 93 of file x509.py.

**10.178.3 Member Data Documentation****10.178.3.1 rpki.x509.PEM\_converter.b**

Definition at line 70 of file x509.py.

**10.178.3.2 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 \(2481\)](#)

## 10.179 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](#).*

### 10.179.1 Detailed Description

Class to hold a PKCS #10 request.

Definition at line 481 of file x509.py.

### 10.179.2 Member Function Documentation

#### 10.179.2.1 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 516 of file x509.py.

#### 10.179.2.2 `def rpki.x509.PKCS10.create ( cls, keypair, exts = None)`

Create a new request for a given keypair, including given extensions.

Definition at line 576 of file x509.py.

#### 10.179.2.3 `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 563 of file x509.py.

#### 10.179.2.4 `def rpki.x509.PKCS10.get_DER ( self)`

Get the DER value of this certification request.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 489 of file x509.py.

#### 10.179.2.5 `def rpki.x509.PKCS10.get_POWpkix ( self)`

Get the POW.pkix value of this certification request.

Definition at line 501 of file x509.py.

### 10.179.2.6 def rpki.x509.PKCS10.getPublicKey ( *self* )

Extract the public key from this certification request.

Definition at line 512 of file x509.py.

## 10.179.3 Member Data Documentation

### 10.179.3.1 rpki.x509.PKCS10.DER

DER value of this [object](#).

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 497 of file x509.py.

### 10.179.3.2 tuple rpki.x509.PKCS10.formats = ("DER", "POWpkix") [static]

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 486 of file x509.py.

### 10.179.3.3 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 487 of file x509.py.

### 10.179.3.4 rpki.x509.PKCS10.POWpkix

Definition at line 509 of file x509.py.

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

- [x509.py \(2481\)](#)

## 10.180 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](#).*

### 10.180.1 Detailed Description

Class to hold a signed ROA.

Definition at line 963 of file x509.py.

### 10.180.2 Member Function Documentation

#### 10.180.2.1 def rpki.x509.ROA.build ( cls, as\_number, ipv4, ipv6, keypair, certs, version = 0)

Build a ROA.

Definition at line 973 of file x509.py.

### 10.180.3 Member Data Documentation

#### 10.180.3.1 rpki.x509.ROA.content\_class = rpki.roa.RouteOriginAttestation [static]

Definition at line 969 of file x509.py.

**10.180.3.2** tuple rpki.x509.ROA.econtent\_oid = POWify\_OID("id-ct-routeOriginAttestation") [static]

Reimplemented from [rpki.x509.CMS\\_object](#).

Definition at line 970 of file x509.py.

**10.180.3.3** 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 968 of file x509.py.

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

- [x509.py \(2481\)](#)

## 10.181 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](#)
- def [get\\_tlslite](#)

### Public Attributes

- [DER](#)  
*DER value of this [object](#).*
- [POW](#)
- [tlslite](#)

### Static Public Attributes

- tuple `formats` = ("DER", "POW", "tlslite")  
*Formats supported in this [object](#).*
- tuple `pem_converter` = `PEM_converter`("RSA PRIVATE KEY")  
*PEM converter for this [object](#).*

#### 10.181.1 Detailed Description

Class to hold an RSA key pair.

Definition at line 590 of file x509.py.

#### 10.181.2 Member Function Documentation

##### 10.181.2.1 `def rpki.x509.RSA.generate ( cls, keylength = 2048 )`

Generate a new keypair.

Definition at line 629 of file x509.py.

##### 10.181.2.2 `def rpki.x509.RSA.get_DER ( self )`

Get the DER value of this keypair.

Reimplemented from `rpki.x509.DER_object`.

Definition at line 598 of file x509.py.

##### 10.181.2.3 `def rpki.x509.RSA.get_POW ( self )`

Get the POW value of this keypair.

Definition at line 610 of file x509.py.



**10.181.2.4 def rpki.x509.RSA.get\_public\_DER ( self)**

Get the DER encoding of the public key from this keypair.

Definition at line 636 of file x509.py.

**10.181.2.5 def rpki.x509.RSA.get\_RSAPublic ( self)**

Convert the public key of this keypair into a RSAPublic object.

Definition at line 644 of file x509.py.

**10.181.2.6 def rpki.x509.RSA.get\_SKI ( self)**

Calculate the SKI of this keypair.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 640 of file x509.py.

**10.181.2.7 def rpki.x509.RSA.get\_tslite ( self)**

Get the tslite value of this keypair.

Definition at line 619 of file x509.py.

**10.181.3 Member Data Documentation****10.181.3.1 rpki.x509.RSA.DER**

DER value of this [object](#).

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 606 of file x509.py.

**10.181.3.2** tuple `rpki.x509.RSA.formats` = ("DER", "POW", "tlsite")  
[static]

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 595 of file x509.py.

**10.181.3.3** 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 596 of file x509.py.

**10.181.3.4** `rpki.x509.RSA.POW`

Definition at line 616 of file x509.py.

**10.181.3.5** `rpki.x509.RSA.tlsite`

Definition at line 625 of file x509.py.

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

- [x509.py](#) (2481)

## 10.182 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](#).*

#### 10.182.1 Detailed Description

Class to hold an RSA public key.

Definition at line 648 of file x509.py.

#### 10.182.2 Member Function Documentation

##### 10.182.2.1 def rpki.x509.RSAPublic.get\_DER ( *self*)

Get the DER value of this public key.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 656 of file x509.py.

##### 10.182.2.2 def rpki.x509.RSAPublic.get\_POW ( *self*)

Get the POW value of this public key.

Definition at line 668 of file x509.py.

**10.182.2.3 def rpki.x509.RSAPublic.get\_SKI ( *self* )**

Calculate the SKI of this public key.

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 677 of file x509.py.

**10.182.3 Member Data Documentation****10.182.3.1 rpki.x509.RSAPublic.DER**

DER value of this [object](#).

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 664 of file x509.py.

**10.182.3.2 tuple rpki.x509.RSAPublic.formats = ("DER", "POW")  
[static]**

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 653 of file x509.py.

**10.182.3.3 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 654 of file x509.py.

**10.182.3.4 rpki.x509.RSAPublic.POW**

Definition at line 674 of file x509.py.

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

- [x509.py \(2481\)](#)

## 10.183 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](#).*

### 10.183.1 Detailed Description

Class to hold a signed manifest.

Definition at line 923 of file x509.py.

### 10.183.2 Member Function Documentation

#### 10.183.2.1 def rpki.x509.SignedManifest.build ( cls, serial, thisUpdate, nextUpdate, names\_and\_objs, keypair, certs, version = 0)

Build a signed manifest.

Definition at line 941 of file x509.py.

**10.183.2.2 def rpki.x509.SignedManifest.getNextUpdate ( *self* )**

Get nextUpdate value from this manifest.

Definition at line 936 of file x509.py.

**10.183.2.3 def rpki.x509.SignedManifest.getThisUpdate ( *self* )**

Get thisUpdate value from this manifest.

Definition at line 932 of file x509.py.

**10.183.3 Member Data Documentation****10.183.3.1 rpki.x509.SignedManifest.content\_class = rpki.manifest.Manifest  
[static]**

Definition at line 929 of file x509.py.

**10.183.3.2 tuple rpki.x509.SignedManifest.econtent\_oid =  
POWify\_OID("id-ct-rpkiManifest") [static]**

Reimplemented from [rpki.x509.CMS\\_object](#).

Definition at line 930 of file x509.py.

**10.183.3.3 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 928 of file x509.py.

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

- [x509.py](#) (2481)

## 10.184 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 [get\\_tslite](#)
- 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](#)
- [tslite](#)

### Static Public Attributes

- tuple [formats](#) = ("DER", "[POW](#)", "[POWpkix](#)", "[tslite](#)")  
*Formats supported in this [object](#).*
- tuple [pem\\_converter](#) = [PEM\\_converter](#)("CERTIFICATE")  
*PEM converter for this [object](#).*

### 10.184.1 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.

### 10.184.2 Member Function Documentation

#### 10.184.2.1 def rpki.x509.X509.expired ( self)

Test whether this certificate has expired.

Definition at line 408 of file x509.py.

#### 10.184.2.2 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.

#### 10.184.2.3 def rpki.x509.X509.get\_POW ( self)

Get the POW value of this certificate.

Definition at line 353 of file x509.py.

#### 10.184.2.4 def rpki.x509.X509.get\_POWpkix ( self)

Get the POW.pkix value of this certificate.

Definition at line 362 of file x509.py.



**10.184.2.5 def rpki.x509.X509.get\_tslite ( *self* )**

Get the tslite value of this certificate.

Definition at line 373 of file x509.py.

**10.184.2.6 def rpki.x509.X509.getIssuer ( *self* )**

Get the issuer of this certificate.

Definition at line 384 of file x509.py.

**10.184.2.7 def rpki.x509.X509.getNotAfter ( *self* )**

Get the expiration time of this certificate.

Definition at line 396 of file x509.py.

**10.184.2.8 def rpki.x509.X509.getNotBefore ( *self* )**

Get the inception time of this certificate.

Definition at line 392 of file x509.py.

**10.184.2.9 def rpki.x509.X509.getPublicKey ( *self* )**

Extract the public key from this certificate.

Definition at line 404 of file x509.py.

**10.184.2.10 def rpki.x509.X509.getSerial ( self)**

Get the serial number of this certificate.

Definition at line 400 of file x509.py.

**10.184.2.11 def rpki.x509.X509.getSubject ( self)**

Get the subject of this certificate.

Definition at line 388 of file x509.py.

**10.184.2.12 def rpki.x509.X509.issue ( self, keypair, subject\_key, serial, sia, aia, crldp, notAfter, cn = None, resources = None, is\_ca = True)**

Issue a certificate.

Definition at line 412 of file x509.py.

**10.184.2.13 def rpki.x509.X509.normalize\_chain ( cls, chain)**

Normalize a chain of certificates into a tuple of X509 objects. Given all the glue certificates needed for BPKI cross certification, it's easiest to allow sloppy arguments to the HTTPS and CMS validation methods and provide a single method that normalizes the allowed cases. So this method allows X509, None, lists, and tuples, and returns a tuple of X509 objects.

Definition at line 468 of file x509.py.

**10.184.3 Member Data Documentation****10.184.3.1 rpki.x509.X509.DER**

DER value of this [object](#).

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 340 of file x509.py.

**10.184.3.2** `tuple rpki.x509.X509.formats = ("DER", "POW", "POWpkix", "tlslite")` `[static]`

Formats supported in this [object](#).

Reimplemented from [rpki.x509.DER\\_object](#).

Definition at line 329 of file x509.py.

**10.184.3.3** `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.

**10.184.3.4** `rpki.x509.X509.POW`

Definition at line 359 of file x509.py.

**10.184.3.5** `rpki.x509.X509.POWpkix`

Definition at line 370 of file x509.py.

**10.184.3.6** `rpki.x509.X509.tlslite`

Definition at line 381 of file x509.py.

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

- [x509.py \(2481\)](#)

## 10.185 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")

#### 10.185.1 Detailed Description

Class to hold CMS-wrapped XML protocol data.

Definition at line 986 of file x509.py.

#### 10.185.2 Member Function Documentation

##### 10.185.2.1 def rpki.x509.XML\_CMS\_object.decode ( *self*, *xml* )

Decode XML and set inner content.

Definition at line 1011 of file x509.py.

**10.185.2.2 def rpki.x509.XML\_CMS\_object.dump\_to\_disk ( self, prefix)**

Write DER of current message to disk, for debugging.

Definition at line 1029 of file x509.py.

**10.185.2.3 def rpki.x509.XML\_CMS\_object.encode ( self)**

Encode inner content for signing.

Definition at line 1007 of file x509.py.

**10.185.2.4 def rpki.x509.XML\_CMS\_object.pretty\_print\_content ( self)**

Pretty print XML content of this message.

Definition at line 1015 of file x509.py.

**10.185.2.5 def rpki.x509.XML\_CMS\_object.schema\_check ( self)**

Handle XML RelaxNG schema check.

Definition at line 1019 of file x509.py.

**10.185.2.6 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 1055 of file x509.py.

**10.185.2.7** `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 1038 of file x509.py.

### 10.185.3 Member Data Documentation

#### 10.185.3.1 rpki.x509.XML\_CMS\_object.content

Reimplemented from [rpki.x509.CMS\\_object](#).

Definition at line 1013 of file x509.py.

**10.185.3.2** `rpki.x509.XML_CMS_object.dump_inbound_cms = None`  
[static]

Definition at line 1005 of file x509.py.

**10.185.3.3** `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 998 of file x509.py.

**10.185.3.4** `tuple rpki.x509.XML_CMS_object.econtent_oid =`  
`POWify_OID("id-ct-xml")` [static]

Reimplemented from [rpki.x509.CMS\\_object](#).

Definition at line 991 of file x509.py.

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

- [x509.py \(2481\)](#)

## 10.186 rpki.xml\_utils.base\_elt Class Reference

Inherits [object](#).

Inherited by [rpki.left\\_right.list\\_resources\\_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.*

### 10.186.1 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`.

## 10.186.2 Member Function Documentation

### 10.186.2.1 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.

### 10.186.2.2 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.

### 10.186.2.3 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.

### 10.186.2.4 def rpki.xml\_utils.base\_elt.make\_elt ( self)

XML element constructor.

Definition at line 178 of file xml\_utils.py.

### 10.186.2.5 def rpki.xml\_utils.base\_elt.make\_pdu ( cls, kargs)

Generic PDU constructor.

Definition at line 208 of file xml\_utils.py.



**10.186.2.6** `def rpki.xml_utils.base_elt.read_attrs (self, attrs)`

Template-driven attribute reader.

Definition at line 166 of file xml\_utils.py.

**10.186.2.7** `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](#), and [rpki.publication.config\\_elt](#).

Definition at line 145 of file xml\_utils.py.

**10.186.2.8** `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.

**10.186.3 Member Data Documentation****10.186.3.1** `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.parent\\_elt](#), [rpki.left\\_right.child\\_elt](#), [rpki.left\\_right.repository\\_elt](#), [rpki.left\\_right.route\\_origin\\_elt](#), [rpki.left\\_right.list\\_resources\\_elt](#), [rpki.left\\_right.report\\_error\\_elt](#), [rpki.publication.config\\_elt](#), [rpki.publication.client\\_elt](#), [rpki.publication.publication\\_object\\_elt](#), and [rpki.publication.report\\_error\\_elt](#).

Definition at line 135 of file xml\_utils.py.

### 10.186.3.2 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](#).

### 10.186.3.3 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.parent\\_elt](#), [rpki.left\\_right.child\\_elt](#), [rpki.left\\_right.repository\\_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 \(2452\)](#)

## 10.187 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](#)

### 10.187.1 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.

### 10.187.2 Member Function Documentation

#### 10.187.2.1 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.

#### 10.187.2.2 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.

#### 10.187.2.3 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.

**10.187.2.4 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.

**10.187.2.5 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.

**10.187.2.6 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.

**10.187.2.7 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.

**10.187.2.8 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.

**10.187.2.9** `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.

**10.187.2.10** `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.

**10.187.2.11** `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](#), [rpki.left\\_right.self\\_elt](#), and [rpki.left\\_right.bsc\\_elt](#).

Definition at line 281 of file xml\_utils.py.

**10.187.2.12** `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.

**10.187.2.13 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.

**10.187.2.14 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 \(2452\)](#)

**10.188 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](#)

### 10.188.1 Detailed Description

Generic top-level PDU.

Definition at line 381 of file xml\_utils.py.

### 10.188.2 Member Function Documentation

#### 10.188.2.1 def rpki.xml\_utils.msg.\_\_str\_\_ ( *self* )

Convert msg object to string.

Definition at line 407 of file xml\_utils.py.

#### 10.188.2.2 def rpki.xml\_utils.msg.endElement ( *self*, *stack*, *name*, *text* )

Handle top-level PDU.

Definition at line 399 of file xml\_utils.py.

#### 10.188.2.3 def rpki.xml\_utils.msg.startElement ( *self*, *stack*, *name*, *attrs* )

Handle top-level PDU.

Definition at line 386 of file xml\_utils.py.

#### 10.188.2.4 def rpki.xml\_utils.msg.toXML ( *self* )

Generate top-level PDU.

Definition at line 411 of file xml\_utils.py.

### 10.188.3 Member Data Documentation

#### 10.188.3.1 `rpki.xml_utils.msg.type`

Definition at line 392 of file `xml_utils.py`.

#### 10.188.3.2 `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` (2452)

### 10.189 `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`



### 10.189.1 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.

### 10.189.2 Member Function Documentation

#### 10.189.2.1 `def rpki.xml_utils.sax_handler.__init__ (self)`

Initialize SAX handler.

Definition at line 53 of file xml\_utils.py.

#### 10.189.2.2 `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.

#### 10.189.2.3 `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.

**10.189.2.4 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.

**10.189.2.5 def rpki.xml\_utils.sax\_handler.endElementNS ( self, name, qname)**

Redirect endElementNS() events to endElement().

Definition at line 65 of file xml\_utils.py.

**10.189.2.6 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.

**10.189.2.7 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.

### 10.189.2.8 `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`.

## 10.189.3 Member Data Documentation

### 10.189.3.1 `rpki.xml_utils.sax_handler.result`

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

### 10.189.3.2 `rpki.xml_utils.sax_handler.stack`

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

### 10.189.3.3 `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 \(2452\)](#)

## 10.190 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 \(2424\)](#)

## 10.191 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 \(2424\)](#)

## 10.192 textwrap.TextWrapper Class Reference

Inherited by [irbe\\_cli.UsageWrapper](#).

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

- [irbe\\_cli.py \(2452\)](#)

## 10.193 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 \(2452\)](#)

# 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.UnexpectedCMSURLs](#)
- 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("rpkid-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](#), [rpkiid\\_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.rpkiid\\_cert](#) = [rpki.x509.X509](#)(Auto\_file = [cfg.get](#)("rpkiid-cert"))
- [irdbd.server\\_cert](#) = [irdbd\\_cert](#),
- tuple [irdbd.startup\\_msg](#) = [cfg.get](#)("startup-message", "")
- tuple [irdbd.u](#) = [urlparse.urlparse](#)([cfg.get](#)("https-url"))

## 11.10 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.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`, 303
- `__call__`
  - `irbe_cli::UsageWrapper`, 113
  - `rpki::async::iterator`, 123
  - `rpki::log::logger`, 213
- `__cmp__`
  - `rpki::async::timer`, 125
  - `rpki::resource_set::resource_range`, 240
  - `rpki::resource_set::roa_prefix`, 255
  - `rpki::x509::DER_object`, 347
- `__eq__`
  - `rpki::resource_set::resource_bag`, 237
- `__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`, 155
  - `rpki::https::http_request`, 158
  - `rpki::https::http_response`, 159
  - `rpki::https::http_server`, 161
  - `rpki::https::http_stream`, 164
  - `rpki::log::logger`, 213
  - `rpki::manifest::FileAndHash`, 214
  - `rpki::manifest::FilesAndHashes`, 215
  - `rpki::manifest::Manifest`, 216
  - `rpki::resource_set::resource_bag`, 237
  - `rpki::resource_set::resource_range`, 240
  - `rpki::resource_set::resource_set`, 246
  - `rpki::resource_set::roa_prefix`, 255
  - `rpki::resource_set::roa_prefix_set`, 259
  - `rpki::roa::ROAIPAddress`, 263
  - `rpki::roa::ROAIPAddresses`, 264
  - `rpki::roa::ROAIPAddressFamilies`, 265
  - `rpki::roa::ROAIPAddressFamily`, 265
  - `rpki::roa::RouteOriginAttestation`, 266
  - `rpki::rpki_engine::child_cert_obj`, 281
  - `rpki::rpki_engine::revoked_cert_obj`, 285
  - `rpki::rpki_engine::rpkid_context`, 288
  - `rpki::sql::session`, 292
  - `rpki::sql::template`, 301
  - `rpki::up_down::class_elt`, 314
  - `rpki::up_down::class_response_-syntax`, 317
  - `rpki::up_down::error_response_pdu`, 320
  - `rpki::up_down::multi_uri`, 331
  - `rpki::x509::DER_object`, 347
  - `rpki::x509::PEM_converter`, 353
  - `rpki::xml_utils::sax_handler`, 385
- `__init__.py(2491)`, 388
- `__ne__`
  - `rpki::resource_set::resource_bag`, 237
- `__new__`
  - `rpki::ipaddrs::v4addr`, 170
  - `rpki::ipaddrs::v6addr`, 171
- `__repr__`
  - `rpki::async::iterator`, 123
  - `rpki::async::timer`, 125
- `__str__`
  - `rpki::https::http_message`, 153
  - `rpki::ipaddrs::v4addr`, 170
  - `rpki::ipaddrs::v6addr`, 171
  - `rpki::resource_set::resource_bag`, 237
  - `rpki::resource_set::resource_range_-as`, 241
  - `rpki::resource_set::resource_range_-`

- ip, 243
- rpki::resource\_set::resource\_set, 246
- rpki::resource\_set::roa\_prefix, 255
- rpki::resource\_set::roa\_prefix\_set, 259
- rpki::sundial::datetime, 304
- rpki::up\_down::message\_pdu, 328
- rpki::up\_down::multi\_uri, 331
- rpki::xml\_utils::base\_elt, 376
- rpki::xml\_utils::msg, 383
- \_sub\_
  - rpki::sundial::datetime, 304
- \_bs2long
  - rpki::resource\_set, 85
- \_comm
  - rpki::resource\_set::resource\_set, 246
- \_exceptions\_enabled
  - rpki::sql::session, 294
- \_long2bs
  - rpki::resource\_set, 85
- \_prefixlen
  - rpki::resource\_set::resource\_range\_ -
    - ip, 243
- \_raiseExitNow
  - rpki::async, 66
- \_rsplit
  - rpki::resource\_set, 85
- \_wrap\_execute
  - rpki::sql::session, 292
- activate
  - rpki::rpki\_engine::ca\_detail\_obj, 269
- address
  - rpki::resource\_set::roa\_prefix, 257
  - rpki::roa::ROAIPAddress, 263
- addresses
  - rpki::roa::ROAIPAddressFamily, 266
- addressFamily
  - rpki::roa::ROAIPAddressFamily, 266
- afi
  - rpki::resource\_set::resource\_set\_ -
    - ipv4, 253
  - rpki::resource\_set::resource\_set\_ -
    - ipv6, 254
- argv
  - irbe\_cli, 50
- as\_number
  - irbe\_cli::route\_origin\_elt, 112
  - rpki::left\_right::route\_origin\_elt, 202
- asID
  - rpki::roa::RouteOriginAttestation, 267
- asn
  - rpki::left\_right::list\_resources\_elt, 186
  - rpki::resource\_set::resource\_bag, 238
- assert\_pristine
  - rpki::sql::session, 292
- async.py(2481), 388
- asynchat::async\_chat, 96
- asyncore::dispatcher, 96
- attributes
  - rpki::left\_right::bsc\_elt, 174
  - rpki::left\_right::child\_elt, 178
  - rpki::left\_right::list\_resources\_elt, 186
  - rpki::left\_right::parent\_elt, 191
  - rpki::left\_right::report\_error\_elt, 193
  - rpki::left\_right::repository\_elt, 196
  - rpki::left\_right::route\_origin\_elt, 202
  - rpki::left\_right::self\_elt, 210
  - rpki::publication::client\_elt, 220
  - rpki::publication::config\_elt, 224
  - rpki::publication::publication\_ -
    - object\_elt, 232
  - rpki::publication::report\_error\_elt, 233
  - rpki::xml\_utils::base\_elt, 377
- b
  - rpki::x509::PEM\_converter, 354
- base\_uri
  - rpki::publication::client\_elt, 220
- bits
  - rpki::ipaddrs::v4addr, 171

- rpki::ipaddr::v6addr, 172
- body
  - rpki::https::http\_message, 154
- booleans
  - rpki::left\_right::bsc\_elt, 174
  - rpki::left\_right::child\_elt, 179
  - rpki::left\_right::parent\_elt, 191
  - rpki::left\_right::route\_origin\_elt, 203
  - rpki::left\_right::self\_elt, 210
  - rpki::xml\_utils::base\_elt, 377
- bpki\_cert
  - irbe\_cli::cmd\_elt\_mixin, 102
  - rpki::left\_right::child\_elt, 179
  - rpki::left\_right::self\_elt, 211
  - rpki::publication::client\_elt, 220
- bpki\_cms\_cert
  - irbe\_cli::cmd\_elt\_mixin, 102
  - rpki::left\_right::parent\_elt, 191
  - rpki::left\_right::repository\_elt, 196
- bpki\_cms\_glue
  - irbe\_cli::cmd\_elt\_mixin, 102
  - rpki::left\_right::parent\_elt, 191
  - rpki::left\_right::repository\_elt, 196
- 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, 211
  - rpki::publication::client\_elt, 220
- bpki\_https\_cert
  - irbe\_cli::cmd\_elt\_mixin, 103
  - rpki::left\_right::parent\_elt, 191
  - rpki::left\_right::repository\_elt, 196
- bpki\_https\_glue
  - irbe\_cli::cmd\_elt\_mixin, 103
  - rpki::left\_right::parent\_elt, 191
  - rpki::left\_right::repository\_elt, 197
- bpki\_ta
  - irbdb, 54
  - pubd::pubd\_context, 116
  - rootd, 61
  - rpki::rpki\_engine::rpkid\_context, 289
- bsc
  - rpki::left\_right::data\_elt, 182
- bscs
  - rpki::left\_right::self\_elt, 207
- buffer
  - rpki::https::http\_stream, 168
- build
  - rpki::x509::ROA, 358
  - rpki::x509::SignedManifest, 365
- build\_https\_ta\_cache
  - pubd::pubd\_context, 115
  - rpki::https, 71
  - rpki::rpki\_engine::rpkid\_context, 288
- ca
  - rpki::rpki\_engine::ca\_detail\_obj, 269
- ca\_cert\_uri
  - rpki::rpki\_engine::ca\_detail\_obj, 273
- ca\_detail
  - rpki::left\_right::route\_origin\_elt, 199
  - rpki::rpki\_engine::child\_cert\_obj, 281
  - rpki::rpki\_engine::revoked\_cert\_obj, 285
- ca\_detail\_id
  - rpki::left\_right::route\_origin\_elt, 203
  - rpki::rpki\_engine::child\_cert\_obj, 283
  - rpki::rpki\_engine::revoked\_cert\_obj, 285
- ca\_details
  - rpki::rpki\_engine::ca\_obj, 276
- ca\_from\_class\_name
  - rpki::left\_right::child\_elt, 177
- ca\_id
  - rpki::rpki\_engine::ca\_detail\_obj, 273
- cache
  - rpki::sql::session, 294
- cache\_clear
  - rpki::sql::session, 292
- calculate\_SKI

- rpki::x509, 93
- call\_daemon
  - irbe\_cli, 50
- call\_pubd
  - rpki::left\_right::repository\_elt, 195
- callback
  - rpki::https::http\_request, 158
- caller\_function
  - rpki::async::iterator, 123
- cancel
  - rpki::async::timer, 125
- cas
  - rpki::left\_right::parent\_elt, 189
- cert
  - cross\_certify, 46
  - rpki::https::http\_client, 148
  - rpki::https::http\_listener, 151
  - rpki::https::http\_queue, 156
  - rpki::left\_right::route\_origin\_elt, 203
  - rpki::rpki\_engine::child\_cert\_obj, 283
  - rpki::up\_down::certificate\_elt, 313
- cert\_url
  - rpki::up\_down::certificate\_elt, 313
  - rpki::up\_down::class\_elt, 315
- certs
  - rpki::up\_down::class\_elt, 315
- cfg
  - irbe\_cli, 50
  - irdbd, 54
  - rootd, 61
- cfg\_file
  - irbe\_cli, 50
  - irdbd, 54
  - pubd, 57
  - rootd, 61
  - rpkid, 95
- characters
  - rpki::xml\_utils::sax\_handler, 385
- check\_allowed\_uri
  - rpki::publication::client\_elt, 218
- check\_for\_updates
  - rpki::rpki\_engine::ca\_obj, 276
- check\_response
  - rpki::up\_down::base\_elt, 310
  - rpki::up\_down::error\_response\_pdu, 320
  - rpki::up\_down::issue\_response\_pdu, 325
- check\_valid\_rpki
  - rpki::x509::PKCS10, 355
- child
  - cross\_certify, 46
  - rpki::rpki\_engine::child\_cert\_obj, 281
- child\_bpki\_cert
  - rootd, 61
- child\_certs
  - rpki::left\_right::child\_elt, 177
  - rpki::rpki\_engine::ca\_detail\_obj, 269
- child\_id
  - rpki::rpki\_engine::child\_cert\_obj, 283
- children
  - rpki::left\_right::bsc\_elt, 173
  - rpki::left\_right::self\_elt, 207
- chunk\_body
  - rpki::https::http\_stream, 164
- 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, 316
  - rpki::up\_down::issue\_pdu, 324
  - rpki::up\_down::revoke\_pdu, 333
  - rpki::up\_down::revoke\_syntax, 335
- classes
  - rpki::up\_down::class\_response\_syntax, 318
- clear
  - rpki::async::timer, 126
  - rpki::x509::DER\_object, 347
- clear\_https\_ta\_cache
  - pubd::pubd\_context, 115
  - rpki::left\_right::child\_elt, 179

- rpki::publication::client\_elt, 220
- rpki::rpki\_engine::rpkid\_context, 288
- client
  - rpki::https, 71
  - rpki::https::http\_queue, 156
- client\_cert
  - irbe\_cli, 50
- client\_getopt
  - irbe\_cli::cmd\_elt\_mixin, 100
- client\_handler
  - pubd::pubd\_context, 115
- client\_key
  - irbe\_cli, 50
- client\_poll
  - rpki::left\_right::self\_elt, 207
- client\_query\_as\_number
  - irbe\_cli::route\_origin\_elt, 111
- client\_query\_bpki\_cert
  - irbe\_cli::cmd\_elt\_mixin, 100
- client\_query\_bpki\_cms\_cert
  - irbe\_cli::cmd\_elt\_mixin, 101
- client\_query\_bpki\_crl
  - irbe\_cli::config\_elt, 105
- client\_query\_bpki\_https\_cert
  - irbe\_cli::cmd\_elt\_mixin, 101
- client\_query\_cms\_glue
  - irbe\_cli::cmd\_elt\_mixin, 101
- client\_query\_glue
  - irbe\_cli::cmd\_elt\_mixin, 101
- client\_query\_https\_glue
  - irbe\_cli::cmd\_elt\_mixin, 101
- client\_query\_ipv4
  - irbe\_cli::route\_origin\_elt, 111
- client\_query\_ipv6
  - irbe\_cli::route\_origin\_elt, 111
- client\_query\_signing\_cert
  - irbe\_cli::bsc\_elt, 97
- client\_query\_signing\_cert\_crl
  - irbe\_cli::bsc\_elt, 97
- client\_queues
  - rpki::https, 72
- client\_reply\_decode
  - irbe\_cli::bsc\_elt, 97
  - irbe\_cli::cmd\_elt\_mixin, 102
- client\_reply\_show
  - irbe\_cli::cmd\_elt\_mixin, 102
- client\_ta
  - irbdb, 54
  - rootd, 61
- close
  - rpki::https::http\_stream, 165
  - rpki::sql::session, 292
- cmd
  - rpki::https::http\_request, 158
- cms\_class
  - irbe\_cli, 51
- code
  - rpki::https::http\_response, 160
- codes
  - rpki::up\_down::error\_response\_pdu, 321
- collect\_incoming\_data
  - rpki::https::http\_stream, 165
- columns
  - rpki::sql::template, 301
- compose\_response
  - rootd, 60
- config.py(2452), 389
- config\_id
  - rpki::publication::config\_elt, 224
- ConfigParser::RawConfigParser, 96
- connect
  - rpki::sql::session, 293
- construct\_sia\_uri
  - rpki::rpki\_engine::ca\_obj, 276
- contains
  - rpki::resource\_set::resource\_set, 247
- content
  - rpki::x509::CMS\_object, 339
  - rpki::x509::DER\_CMS\_object, 346
  - rpki::x509::XML\_CMS\_object, 374
- content\_class
  - rpki::x509::ROA, 358
  - rpki::x509::SignedManifest, 366
- control\_handler
  - pubd::pubd\_context, 115
- convert\_to\_seconds
  - rpki::sundial::timedelta, 308
- create
  - rpki::rpki\_engine::ca\_detail\_obj, 269



- rpki::rpki\_engine::ca\_obj, 276
- rpki::x509::PKCS10, 356
- create\_ca
  - rpki::x509::PKCS10, 356
- create\_top\_level
  - rpki::xml\_utils::sax\_handler, 385
- critical
  - cross\_certify, 46
- crl\_interval
  - rpki::left\_right::self\_elt, 211
- crl\_uri
  - rpki::rpki\_engine::ca\_detail\_obj, 269
- crl\_uri\_tail
  - rpki::rpki\_engine::ca\_detail\_obj, 269
- cronjob\_handler
  - rpki::rpki\_engine::rpkid\_context, 288
- cross\_certify, 44
  - cert, 46
  - child, 46
  - critical, 46
  - f, 46
  - keypair, 46
  - lifetime, 46
  - make\_ext, 45
  - notAfter, 46
  - now, 47
  - output, 47
  - parent, 47
  - serial, 47
  - serial\_file, 47
  - usage, 46
  - value, 47
  - x, 47
- cross\_certify.py(2433), 389
- cur
  - irdbd, 54
  - rpki::sql::session, 294
- database
  - rpki::sql::session, 294
- datum\_type
  - rpki::resource\_set::resource\_range\_as, 242
- rpki::resource\_set::resource\_range\_ipv4, 244
- rpki::resource\_set::resource\_range\_ipv6, 245
- db
  - irdbd, 54
  - rpki::sql::session, 294
- debug
  - rpki::https, 72
  - rpki::log, 77
- debug\_cms\_certs
  - rpki::x509::CMS\_object, 339
- debug\_tls\_certs
  - rpki::https, 72
- decode
  - rpki::x509::DER\_CMS\_object, 345
  - rpki::x509::XML\_CMS\_object, 372
- default\_http\_version
  - rpki::https, 72
- default\_section
  - rpki::config::parser, 130
- default\_timeout
  - rpki::https, 72
- del\_subject\_cert
  - rootd, 60
- delete
  - rpki::rpki\_engine::ca\_detail\_obj, 270
  - rpki::rpki\_engine::ca\_obj, 277
  - rpki::sql::template, 301
- DER
  - rpki::x509::CMS\_object, 339
  - rpki::x509::CRL, 344
  - rpki::x509::DER\_object, 352
  - rpki::x509::PKCS10, 357
  - rpki::x509::RSA, 361
  - rpki::x509::RSAPublic, 364
  - rpki::x509::X509, 370
- description
  - rpki::up\_down::error\_response\_pdu, 321
- detach
  - rpki::https::http\_queue, 155
- difference
  - rpki::resource\_set::resource\_set, 247
- dirty

- rpki::sql::session, 294
- done\_callback
  - rpki::async::iterator, 123
- dump\_inbound\_cms
  - rpki::x509::XML\_CMS\_object, 374
- dump\_on\_verify\_failure
  - rpki::x509::CMS\_object, 339
- dump\_outbound\_cms
  - rpki::x509::XML\_CMS\_object, 374
- dump\_to\_disk
  - rpki::x509::XML\_CMS\_object, 372
- dumpasn1
  - rpki::x509::DER\_object, 348
- dynamic\_ta
  - rpki::https::http\_listener, 151
- e
  - rpki::x509::PEM\_converter, 354
- earlier
  - rpki::sundial::datetime, 304
- econtent\_oid
  - rpki::x509::CMS\_object, 340
  - rpki::x509::ROA, 358
  - rpki::x509::SignedManifest, 366
  - rpki::x509::XML\_CMS\_object, 374
- ee\_uri
  - rpki::left\_right::route\_origin\_elt, 199
- ee\_uri\_tail
  - rpki::left\_right::route\_origin\_elt, 199
- element\_name
  - rpki::left\_right::bsc\_elt, 175
  - rpki::left\_right::child\_elt, 179
  - rpki::left\_right::list\_resources\_elt, 186
  - rpki::left\_right::parent\_elt, 192
  - rpki::left\_right::report\_error\_elt, 194
  - rpki::left\_right::repository\_elt, 197
  - rpki::left\_right::route\_origin\_elt, 203
  - rpki::left\_right::self\_elt, 211
  - rpki::publication::certificate\_elt, 217
  - rpki::publication::client\_elt, 220
  - rpki::publication::config\_elt, 224
  - rpki::publication::crl\_elt, 226
  - rpki::publication::manifest\_elt, 227
  - rpki::publication::report\_error\_elt, 233
  - rpki::publication::roa\_elt, 234
- elements
  - rpki::left\_right::bsc\_elt, 175
  - rpki::left\_right::child\_elt, 179
  - rpki::left\_right::parent\_elt, 192
  - rpki::left\_right::repository\_elt, 197
  - rpki::left\_right::self\_elt, 211
  - rpki::publication::client\_elt, 220
  - rpki::publication::config\_elt, 224
  - rpki::xml\_utils::base\_elt, 378
- empty
  - rpki::resource\_set::resource\_bag, 237
  - rpki::x509::DER\_object, 348
- enable\_trace
  - rpki::log, 77
- encode
  - rpki::x509::DER\_CMS\_object, 345
  - rpki::x509::XML\_CMS\_object, 373
- encoding
  - rpki::left\_right::cms\_msg, 180
  - rpki::publication::cms\_msg, 222
  - rpki::up\_down::cms\_msg, 319
- endElement
  - rpki::left\_right::child\_elt, 177
  - rpki::publication::client\_elt, 218
  - rpki::publication::publication\_object\_elt, 231
  - rpki::up\_down::base\_elt, 310
  - rpki::up\_down::certificate\_elt, 312
  - rpki::up\_down::class\_elt, 314
  - rpki::up\_down::error\_response\_pdu, 320
  - rpki::up\_down::issue\_pdu, 323
  - rpki::xml\_utils::base\_elt, 376
  - rpki::xml\_utils::data\_elt, 379
  - rpki::xml\_utils::msg, 383
  - rpki::xml\_utils::sax\_handler, 385
- endElementNS
  - rpki::xml\_utils::sax\_handler, 386
- enforce\_strict\_up\_down\_xml\_sender
  - rpki::left\_right, 75
- errback

- rpki::async::timer, 126, 128
- rpki::https::http\_request, 158
- error
  - rpki::log, 77
- error\_code
  - rpki::left\_right::report\_error\_elt, 194
  - rpki::publication::report\_error\_elt, 234
- event\_loop
  - rpki::async, 66
- Exception, 96
- exceptions
  - rpki::up\_down::error\_response\_pdu, 321
- exceptions.py(2452), 390
- excludes
  - irbe\_cli::bsc\_elt, 98
  - irbe\_cli::cmd\_elt\_mixin, 103
- execute
  - rpki::sql::session, 293
- executemany
  - rpki::sql::session, 293
- exit\_event\_loop
  - rpki::async, 66
- ExitNow
  - rpki::async, 67
- expect\_close
  - rpki::https::http\_client, 148
  - rpki::https::http\_server, 162
- expired
  - rpki::x509::X509, 368
- expires
  - rpki::rpki\_engine::revoked\_cert\_obj, 285
- explicitVersion
  - rpki::manifest::Manifest, 216
  - rpki::roa::RouteOriginAttestation, 267
- extract
  - rpki::x509::CMS\_object, 337
- f
  - cross\_certify, 46
- fetch
  - rpki::publication::config\_elt, 223
  - rpki::rpki\_engine::child\_cert\_obj, 282
- fetch\_active
  - rpki::rpki\_engine::ca\_obj, 277
- fetch\_deprecated
  - rpki::rpki\_engine::ca\_obj, 277
- fetch\_pending
  - rpki::rpki\_engine::ca\_obj, 277
- fetch\_revoked
  - rpki::rpki\_engine::ca\_obj, 277
- fetchall
  - rpki::sql::session, 293
- file
  - rpki::manifest::FileAndHash, 214
- fileHashAlg
  - rpki::manifest::Manifest, 216
- fileList
  - rpki::manifest::Manifest, 216
- find\_handler
  - rpki::https::http\_server, 161
- format
  - rpki::https::http\_message, 153
- format\_first\_line
  - rpki::https::http\_request, 158
  - rpki::https::http\_response, 159
- formats
  - rpki::x509::CMS\_object, 340
  - rpki::x509::CRL, 344
  - rpki::x509::DER\_object, 352
  - rpki::x509::PKCS10, 357
  - rpki::x509::RSA, 361
  - rpki::x509::RSAPublic, 364
  - rpki::x509::X509, 371
- found\_terminator
  - rpki::https::http\_stream, 165
- from\_bytes
  - rpki::ipaddr::v4addr, 170
  - rpki::ipaddr::v6addr, 172
- from\_exception
  - rpki::left\_right::report\_error\_elt, 193
  - rpki::publication::report\_error\_elt, 233
- from\_resource\_bag
  - rpki::up\_down::class\_elt, 315
- from\_rfc3779\_tuples

- rpki::resource\_set::resource\_bag,  
237
- from\_sql
  - rpki::resource\_set::resource\_set, 247
  - rpki::resource\_set::roa\_prefix\_set,  
259
  - rpki::sundial::datetime, 304
  - rpki::x509::DER\_object, 348
- fromASN1tuple
  - rpki::sundial::datetime, 304
- fromdatetime
  - rpki::sundial::datetime, 304
- fromGeneralizedTime
  - rpki::sundial::datetime, 305
- fromtimedelta
  - rpki::sundial::timedelta, 308
- fromUTCTime
  - rpki::sundial::datetime, 305
- fromXMLtime
  - rpki::sundial::datetime, 305
- gAKI
  - rpki::x509::DER\_object, 348
- gctx
  - rpki::rpki\_engine::ca\_detail\_obj,  
273
  - rpki::rpki\_engine::ca\_obj, 279
  - rpki::rpki\_engine::child\_cert\_obj,  
283
  - rpki::rpki\_engine::revoked\_cert\_obj,  
286
  - rpki::sql::sql\_persistent, 300
- generate
  - rpki::x509::CRL, 342
  - rpki::x509::RSA, 360
- generate\_crl
  - rpki::rpki\_engine::ca\_detail\_obj,  
270
- generate\_manifest
  - rpki::rpki\_engine::ca\_detail\_obj,  
270
- generate\_manifest\_cert
  - rpki::rpki\_engine::ca\_detail\_obj,  
270
- generate\_roa
  - rpki::left\_right::route\_origin\_elt,  
199
- get
  - rpki::config::parser, 129
- get\_3779resources
  - rpki::x509::DER\_object, 348
- get\_AIA
  - rpki::x509::DER\_object, 349
- get\_AKI
  - rpki::x509::DER\_object, 349
- get\_Base64
  - rpki::x509::DER\_object, 349
- get\_basicConstraints
  - rpki::x509::DER\_object, 349
- get\_buffer
  - rpki::https::http\_stream, 165
- get\_content
  - rpki::x509::CMS\_object, 338
- get\_DER
  - rpki::x509::CMS\_object, 338
  - rpki::x509::CRL, 342
  - rpki::x509::DER\_object, 349
  - rpki::x509::PKCS10, 356
  - rpki::x509::RSA, 360
  - rpki::x509::RSAPublic, 363
  - rpki::x509::X509, 368
- get\_PEM
  - rpki::x509::DER\_object, 350
- get\_POW
  - rpki::x509::CMS\_object, 338
  - rpki::x509::CRL, 342
  - rpki::x509::RSA, 360
  - rpki::x509::RSAPublic, 363
  - rpki::x509::X509, 368
- get\_POWpkix
  - rpki::x509::CRL, 343
  - rpki::x509::PKCS10, 356
  - rpki::x509::X509, 368
- get\_public\_DER
  - rpki::x509::RSA, 360
- get\_RSAPublic
  - rpki::x509::RSA, 361
- get\_SIA
  - rpki::x509::DER\_object, 350
- get\_SKI
  - rpki::up\_down::revoke\_pdu, 332

- rpki::x509::DER\_object, 350
- rpki::x509::RSA, 361
- rpki::x509::RSAPublic, 363
- get\_subject\_cert
  - rootd, 60
- get\_subject\_pkcs10
  - rootd, 60
- get\_tlslite
  - rpki::x509::RSA, 361
  - rpki::x509::X509, 368
- getIssuer
  - rpki::x509::CRL, 343
  - rpki::x509::X509, 369
- getNextUpdate
  - rpki::x509::CRL, 343
  - rpki::x509::SignedManifest, 365
- getNotAfter
  - rpki::x509::X509, 369
- getNotBefore
  - rpki::x509::X509, 369
- getPublicKey
  - rpki::x509::PKCS10, 356
  - rpki::x509::X509, 369
- getSerial
  - rpki::x509::X509, 369
- getSubject
  - rpki::x509::X509, 370
- getThisUpdate
  - rpki::x509::CRL, 343
  - rpki::x509::SignedManifest, 366
- gSKI
  - rpki::x509::DER\_object, 350
- hAKI
  - rpki::x509::DER\_object, 351
- 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, 147
  - rpki::https::http\_server, 161
- handle\_no\_content\_length
  - rpki::https::http\_client, 147
  - rpki::https::http\_server, 161
- handle\_read
  - rpki::https::http\_stream, 166
- handle\_timeout
  - rpki::https::http\_client, 147
  - rpki::https::http\_stream, 166
- handle\_write
  - rpki::https::http\_stream, 166
- handler
  - irdbd, 54
  - rpki::async::timer, 126, 128
- handler\_common
  - pubd::pubd\_context, 115
- handlers
  - irdbd, 55
  - rootd, 61
  - rpki::https::http\_listener, 151
  - rpki::https::http\_server, 162
- hash
  - rpki::manifest::FileAndHash, 214
- headers
  - rpki::https::http\_message, 154
- host
  - irdbd, 55
  - rootd, 61
- hostport
  - rpki::https::http\_client, 148
  - rpki::https::http\_queue, 156
- hSKI
  - rpki::x509::DER\_object, 351
- https.py(2486), 391
- https\_server\_host
  - pubd::pubd\_context, 116
  - rootd, 62
  - rpki::rpki\_engine::rpkid\_context, 289
- https\_server\_port
  - pubd::pubd\_context, 116
  - rootd, 62

- rpki::rpki\_engine::rpkid\_context, 289
- https\_ta\_cache
  - pubd::pubd\_context, 116
  - rpki::rpki\_engine::rpkid\_context, 289
- ignore
  - rpki::async::iterator, 123
- index
  - rpki::sql::template, 302
- info
  - rpki::log, 77
- inherit
  - rpki::resource\_set::resource\_set, 249
  - rpki::resource\_set::resource\_set\_as, 250
  - rpki::resource\_set::resource\_set\_ip, 252
- inherit\_token
  - rpki::resource\_set, 86
- init
  - rpki::log, 76
- initate\_send
  - rpki::https::http\_stream, 166
- insert
  - rpki::sql::template, 302
- intersection
  - rpki::resource\_set::resource\_bag, 237
  - rpki::resource\_set::resource\_set, 247
- ipAddrBlocks
  - rpki::roa::RouteOriginAttestation, 267
- ipaddrs.py(2424), 392
- ipv4
  - irbe\_cli::route\_origin\_elt, 112
  - rpki::left\_right::list\_resources\_elt, 186
  - rpki::left\_right::route\_origin\_elt, 203
- ipv6
  - irbe\_cli::route\_origin\_elt, 112
  - rpki::left\_right::list\_resources\_elt, 186
- rpki::left\_right::route\_origin\_elt, 204
- irbe\_cert
  - pubd::pubd\_context, 116
  - rpki::rpki\_engine::rpkid\_context, 289
- irbe\_cli, 48
  - argv, 50
  - call\_daemon, 50
  - cfg, 50
  - cfg\_file, 50
  - client\_cert, 50
  - client\_key, 50
  - cms\_class, 51
  - pem\_out, 51
  - q\_msg, 51
  - q\_msg\_left\_right, 51
  - q\_msg\_publication, 51
  - q\_pdu, 51
  - server\_ta, 51
  - top\_opts, 52
  - url, 52
  - usage, 50
  - usage\_fill, 52
  - verbose, 52
- irbe\_cli.py(2452), 392
- irbe\_cli::bsc\_elt, 96
  - client\_query\_signing\_cert, 97
  - client\_query\_signing\_cert\_crl, 97
  - client\_reply\_decode, 97
  - excludes, 98
  - signing\_cert, 98
  - signing\_cert\_crl, 98
- irbe\_cli::certificate\_elt, 98
- irbe\_cli::child\_elt, 99
- irbe\_cli::client\_elt, 99
- irbe\_cli::cmd\_elt\_mixin, 99
  - bpki\_cert, 102
  - bpki\_cms\_cert, 102
  - bpki\_cms\_glue, 102
  - bpki\_glue, 103
  - bpki\_https\_cert, 103
  - bpki\_https\_glue, 103
  - client\_getopt, 100
  - client\_query\_bpki\_cert, 100
  - client\_query\_bpki\_cms\_cert, 101

- client\_query\_bpki\_https\_cert, 101
- client\_query\_cms\_glue, 101
- client\_query\_glue, 101
- client\_query\_https\_glue, 101
- client\_reply\_decode, 102
- client\_reply\_show, 102
- excludes, 103
- usage, 102
- irbe\_cli::cmd\_msg\_mixin, 103
- usage, 104
- irbe\_cli::config\_elt, 104
- bpki\_crl, 105
- client\_query\_bpki\_crl, 105
- irbe\_cli::crl\_elt, 105
- irbe\_cli::left\_right\_cms\_msg, 105
- saxify, 106
- irbe\_cli::left\_right\_msg, 106
- pdu, 106
- irbe\_cli::left\_right\_sax\_handler, 107
- pdu, 107
- irbe\_cli::manifest\_elt, 107
- irbe\_cli::parent\_elt, 108
- irbe\_cli::publication\_cms\_msg, 108
- saxify, 108
- irbe\_cli::publication\_msg, 109
- pdu, 109
- irbe\_cli::publication\_sax\_handler, 109
- 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, 111
- ipv4, 112
- ipv6, 112
- irbe\_cli::self\_elt, 112
- irbe\_cli::UsageWrapper, 113
- \_\_call\_\_, 113
- irdb\_cert
- rpki::rpki\_engine::rpkid\_context, 290
- irdb\_query
- rpki::rpki\_engine::rpkid\_context, 288
- irdb\_url
- rpki::rpki\_engine::rpkid\_context, 290
- irdbd, 52
- bpki\_ta, 54
- cfg, 54
- cfg\_file, 54
- client\_ta, 54
- cur, 54
- db, 54
- handler, 54
- handlers, 55
- host, 55
- irdbd\_cert, 55
- irdbd\_key, 55
- port, 55
- rpkid\_cert, 55
- server\_cert, 55
- startup\_msg, 56
- u, 56
- irdbd.py(2491), 393
- irdbd\_cert
- irdbd, 55
- irdbd\_key
- irdbd, 55
- is\_CA
- rpki::x509::DER\_object, 351
- is\_set
- rpki::async::timer, 126
- issubset
- rpki::resource\_set::resource\_set, 248
- issue
- rpki::rpki\_engine::ca\_detail\_obj, 270
- rpki::x509::X509, 370
- issue\_ee
- rpki::rpki\_engine::ca\_detail\_obj, 271
- issue\_subject\_cert\_maybe
- rootd, 60
- issuer
- rpki::up\_down::class\_elt, 316
- issuperset
- rpki::resource\_set::resource\_set, 248
- item\_callback
- rpki::async::iterator, 124

- iterator
  - rpki::async::iterator, [124](#)
- key
  - rpki::https::http\_client, [149](#)
  - rpki::https::http\_listener, [151](#)
  - rpki::https::http\_queue, [156](#)
- keypair
  - cross\_certify, [46](#)
- last\_crl\_sn
  - rpki::rpki\_engine::ca\_obj, [279](#)
- last\_issued\_sn
  - rpki::rpki\_engine::ca\_obj, [279](#)
- last\_manifest\_sn
  - rpki::rpki\_engine::ca\_obj, [279](#)
- lastrowid
  - rpki::sql::session, [293](#)
- later
  - rpki::sundial::datetime, [305](#)
- latest\_ca\_cert
  - rpki::rpki\_engine::ca\_detail\_obj, [273](#)
- latest\_crl
  - rpki::rpki\_engine::ca\_detail\_obj, [273](#)
- latest\_manifest
  - rpki::rpki\_engine::ca\_detail\_obj, [273](#)
- latest\_manifest\_cert
  - rpki::rpki\_engine::ca\_detail\_obj, [273](#)
- left\_right
  - rpki::relaxng, [82](#)
- left\_right.py(2491), [394](#)
- left\_right\_handler
  - rpki::rpki\_engine::rpkid\_context, [288](#)
- lifetime
  - cross\_certify, [46](#)
- log
  - rpki::https::http\_listener, [152](#)
  - rpki::https::http\_queue, [156](#)
  - rpki::https::http\_stream, [168](#)
- log.py(2452), [395](#)
- log\_cert
  - rpki::https::http\_stream, [167](#)
- logger
  - rpki::https, [71](#)
- long, [113](#)
- looks\_like\_PEM
  - rpki::x509::PEM\_converter, [353](#)
- main
  - pubd, [57](#)
  - rpkid, [95](#)
- make\_b64elt
  - rpki::up\_down::base\_elt, [310](#)
  - rpki::xml\_utils::base\_elt, [376](#)
- make\_elt
  - rpki::up\_down::base\_elt, [310](#)
  - rpki::xml\_utils::base\_elt, [376](#)
- make\_ext
  - cross\_certify, [45](#)
- make\_pdu
  - rpki::xml\_utils::base\_elt, [376](#)
- make\_prefix
  - rpki::resource\_set::resource\_range\_ip, [243](#)
- make\_query
  - rpki::up\_down::message\_pdu, [328](#)
- make\_reply
  - rpki::xml\_utils::data\_elt, [379](#)
- make\_reply\_clone\_hook
  - rpki::left\_right::data\_elt, [182](#)
  - rpki::xml\_utils::data\_elt, [379](#)
- manifest.py(2424), [395](#)
- manifest\_private\_key\_id
  - rpki::rpki\_engine::ca\_detail\_obj, [273](#)
- manifest\_public\_key
  - rpki::rpki\_engine::ca\_detail\_obj, [274](#)
- manifest\_uri
  - rpki::rpki\_engine::ca\_detail\_obj, [271](#)
- manifestNumber
  - rpki::manifest::Manifest, [216](#)
- map
  - rpki::sql::template, [302](#)
- max



- rpki::resource\_set::resource\_range, 240
- rpki::resource\_set::roa\_prefix, 256
- max\_prefixlen
  - rpki::resource\_set::roa\_prefix, 257
- maxLength
  - rpki::roa::ROAIPAddress, 263
- min
  - rpki::resource\_set::resource\_range, 240
  - rpki::resource\_set::resource\_range\_as, 242
  - rpki::resource\_set::roa\_prefix, 256
- msg
  - rpki::https::http\_stream, 168
- multiget
  - rpki::config::parser, 129
- name
  - rpki::left\_right::sax\_handler, 205
  - rpki::publication::sax\_handler, 235
  - rpki::up\_down::sax\_handler, 335
- name2oid
  - rpki::oids, 80
- name2type
  - rootd::message\_pdu, 120
  - rpki::up\_down::message\_pdu, 329
- next\_crl\_number
  - rpki::rpki\_engine::ca\_obj, 278
- next\_manifest\_number
  - rpki::rpki\_engine::ca\_obj, 278
- next\_serial\_number
  - rpki::rpki\_engine::ca\_obj, 278
- nextUpdate
  - rpki::manifest::Manifest, 216
  - rpki::rpki\_engine::ca\_detail\_obj, 274
- normalize\_chain
  - rpki::x509::X509, 370
- normalize\_headers
  - rpki::https::http\_message, 153
- notAfter
  - cross\_certify, 46
- note
  - rpki::log, 78
- now
  - cross\_certify, 47
  - rpki::sundial, 90
- nsmapi
  - rpki::left\_right::left\_right\_namespace, 184
  - rpki::publication::publication\_namespace, 229
  - rpki::up\_down, 91
- obj2elt
  - rpki::publication, 82
- object, 113
- oid2name
  - rpki::oids, 80
- oids.py(2424), 396
- other\_clear
  - rpki::x509::CMS\_object, 340
  - rpki::x509::DER\_object, 352
- output
  - cross\_certify, 47
- oversized
  - rpki::resource\_set::resource\_bag, 238
- parent
  - cross\_certify, 47
  - rpki::rpki\_engine::ca\_obj, 278
- parent\_id
  - rpki::rpki\_engine::ca\_obj, 279
- parent\_resource\_class
  - rpki::rpki\_engine::ca\_obj, 280
- parents
  - rpki::left\_right::bsc\_elt, 173
  - rpki::left\_right::child\_elt, 178
  - rpki::left\_right::repository\_elt, 195
  - rpki::left\_right::self\_elt, 207
- parse
  - rpki::sundial::timedelta, 308
- parse\_first\_line
  - rpki::https::http\_request, 158
  - rpki::https::http\_response, 160
- parse\_from\_wire
  - rpki::https::http\_message, 153
- parse\_rfc3779\_tuple
  - rpki::resource\_set::resource\_set\_as, 250

- rpki::resource\_set::resource\_set\_ip, 251
- parse\_str
  - rpki::resource\_set::resource\_set\_as, 250
  - rpki::resource\_set::resource\_set\_ip, 251
  - rpki::resource\_set::roa\_prefix\_set, 260
- parse\_type
  - rpki::https::http\_client, 149
  - rpki::https::http\_server, 162
- parse\_version
  - rpki::https::http\_message, 153
- password
  - rpki::sql::session, 294
- path
  - rpki::https::http\_request, 158
- payload
  - rpki::publication::publication\_object\_elt, 232
  - rpki::up\_down::message\_pdu, 329
- payload\_type
  - rpki::publication::certificate\_elt, 217
  - rpki::publication::crl\_elt, 226
  - rpki::publication::manifest\_elt, 227
  - rpki::publication::roa\_elt, 234
- pdu
  - irbe\_cli::left\_right\_sax\_handler, 107
  - irbe\_cli::publication\_sax\_handler, 110
  - rootd::sax\_handler, 122
  - rpki::left\_right::sax\_handler, 205
  - rpki::publication::sax\_handler, 235
  - rpki::up\_down::sax\_handler, 336
- pdus
  - irbe\_cli::left\_right\_msg, 106
  - irbe\_cli::publication\_msg, 109
  - rpki::left\_right::msg, 188
  - rpki::publication::msg, 228
- pem\_converter
  - rpki::x509::CMS\_object, 340
  - rpki::x509::CRL, 344
  - rpki::x509::DER\_object, 352
  - rpki::x509::PKCS10, 357
  - rpki::x509::ROA, 359
  - rpki::x509::RSA, 362
  - rpki::x509::RSAPublic, 364
  - rpki::x509::SignedManifest, 366
  - rpki::x509::X509, 371
- pem\_out
  - irbe\_cli, 51
- persistent
  - rpki::https::http\_message, 153
- pid
  - rpki::log, 78
- ping
  - rpki::sql::session, 293
- pkcs10
  - rpki::up\_down::issue\_pdu, 324
- pkcs10\_request
  - rpki::left\_right::bsc\_elt, 175
- PKIX\_threshold
  - rpki::sundial::datetime, 307
- port
  - irbdb, 55
  - rootd, 62
- POW
  - rpki::x509::CMS\_object, 341
  - rpki::x509::CRL, 344
  - rpki::x509::RSA, 362
  - rpki::x509::RSAPublic, 364
  - rpki::x509::X509, 371
- POWify\_OID
  - rpki::x509, 93
- POWpkix
  - rpki::x509::CRL, 344
  - rpki::x509::PKCS10, 357
  - rpki::x509::X509, 371
- prefix\_type
  - rpki::resource\_set::roa\_prefix\_set\_ipv4, 261
  - rpki::resource\_set::roa\_prefix\_set\_ipv6, 262
- prefixlen
  - rpki::resource\_set::roa\_prefix, 257
- pretty\_print\_content
  - rpki::x509::XML\_CMS\_object, 373
- print\_on\_der\_error
  - rpki::x509::CMS\_object, 341
- priority
  - rpki::log::logger, 213

- private\_key\_id
  - rpki::left\_right::bsc\_elt, 175
  - rpki::rpki\_engine::ca\_detail\_obj, 274
- profile
  - pubd, 57
  - rpkid, 95
- pubd, 56
  - cfg\_file, 57
  - main, 57
  - profile, 57
- pubd.py(2481), 396
- pubd::pubd\_context, 114
  - \_\_init\_\_, 115
  - bpki\_ta, 116
  - build\_https\_ta\_cache, 115
  - clear\_https\_ta\_cache, 115
  - client\_handler, 115
  - control\_handler, 115
  - handler\_common, 115
  - https\_server\_host, 116
  - https\_server\_port, 116
  - https\_ta\_cache, 116
  - irbe\_cert, 116
  - pubd\_cert, 116
  - pubd\_key, 117
  - publication\_base, 117
  - sql, 117
- pubd\_cert
  - pubd::pubd\_context, 116
- pubd\_key
  - pubd::pubd\_context, 117
- public\_key
  - rpki::rpki\_engine::ca\_detail\_obj, 274
- publication
  - rpki::relaxng, 83
- publication.py(2481), 397
- publication\_base
  - pubd::pubd\_context, 117
- publication\_kludge\_base
  - rpki::rpki\_engine::rpkid\_context, 290
- publish
  - rpki::left\_right::repository\_elt, 195
- publish\_ee\_separately
  - rpki::left\_right::route\_origin\_elt, 204
- pydatetime::datetime, 117
- pydatetime::timedelta, 117
- q\_msg
  - irbe\_cli, 51
- q\_msg\_left\_right
  - irbe\_cli, 51
- q\_msg\_publication
  - irbe\_cli, 51
- q\_pdu
  - irbe\_cli, 51
- query
  - rpki::up\_down::issue\_pdu, 323
  - rpki::up\_down::list\_pdu, 326
  - rpki::up\_down::revoke\_pdu, 332
- query\_up\_down
  - rpki::left\_right::parent\_elt, 189
- queue
  - rpki::async::timer, 128
  - rpki::https::http\_client, 149
  - rpki::https::http\_queue, 157
- range\_type
  - rpki::resource\_set::resource\_set\_as, 250
  - rpki::resource\_set::resource\_set\_ipv4, 253
  - rpki::resource\_set::resource\_set\_ipv6, 254
  - rpki::resource\_set::roa\_prefix\_ipv4, 258
  - rpki::resource\_set::roa\_prefix\_ipv6, 258
- read\_attrs
  - rpki::xml\_utils::base\_elt, 376
- readable
  - rpki::https::http\_stream, 167
- reason
  - rpki::https::http\_response, 160
- recipient
  - rpki::up\_down::message\_pdu, 329
- recv
  - rpki::https::http\_stream, 167
- regen\_margin

- rpki::left\_right::self\_elt, 211
- regenerate\_crls\_and\_manifests
  - rpki::left\_right::self\_elt, 207
- regenerate\_roa
  - rpki::left\_right::route\_origin\_elt, 200
- regex
  - rpki::sundial::timedelta, 308
- reissue
  - rpki::rpki\_engine::child\_cert\_obj, 282
- rekey
  - rpki::rpki\_engine::ca\_obj, 278
- relaxng.py(2492), 397
- repositories
  - rpki::left\_right::bsc\_elt, 174
  - rpki::left\_right::self\_elt, 208
- repository
  - rpki::left\_right::parent\_elt, 190
- req\_resource\_set\_as
  - rpki::up\_down::certificate\_elt, 313
  - rpki::up\_down::issue\_pdu, 324
- req\_resource\_set\_ipv4
  - rpki::up\_down::certificate\_elt, 313
  - rpki::up\_down::issue\_pdu, 324
- req\_resource\_set\_ipv6
  - rpki::up\_down::certificate\_elt, 313
  - rpki::up\_down::issue\_pdu, 324
- request
  - rpki::https::http\_queue, 155
- require\_crls
  - rpki::x509::CMS\_object, 341
- resource\_set.py(2457), 398
- resource\_set\_as
  - rpki::up\_down::class\_elt, 316
- resource\_set\_ipv4
  - rpki::up\_down::class\_elt, 316
- resource\_set\_ipv6
  - rpki::up\_down::class\_elt, 316
- resource\_set\_notafter
  - rpki::up\_down::class\_elt, 316
- resource\_set\_type
  - rpki::resource\_set::roa\_prefix\_set\_ipv4, 261
  - rpki::resource\_set::roa\_prefix\_set\_ipv6, 262
- restart
  - rpki::https::http\_queue, 155
  - rpki::https::http\_stream, 167
- result
  - rpki::xml\_utils::sax\_handler, 387
- retrieved
  - rpki::https::http\_request, 159
- retry\_read
  - rpki::https::http\_client, 149
  - rpki::https::http\_server, 162
  - rpki::https::http\_stream, 168
- retry\_write
  - rpki::https::http\_client, 149
  - rpki::https::http\_server, 163
  - rpki::https::http\_stream, 168
- return\_result
  - rpki::https::http\_queue, 156
- revoke
  - rpki::rpki\_engine::ca\_detail\_obj, 271
  - rpki::rpki\_engine::ca\_obj, 279
  - rpki::rpki\_engine::child\_cert\_obj, 282
  - rpki::rpki\_engine::revoked\_cert\_obj, 285
- revoked
  - rpki::rpki\_engine::revoked\_cert\_obj, 286
- revoked\_certs
  - rpki::rpki\_engine::ca\_detail\_obj, 272
- roa
  - rpki::left\_right::route\_origin\_elt, 204
- roa.py(2424), 399
- roa\_uri
  - rpki::left\_right::route\_origin\_elt, 200
- roa\_uri\_tail
  - rpki::left\_right::route\_origin\_elt, 200
- rootd, 58
  - bpki\_ta, 61
  - cfg, 61
  - cfg\_file, 61
  - child\_bpki\_cert, 61

- client\_ta, 61
- compose\_response, 60
- del\_subject\_cert, 60
- get\_subject\_cert, 60
- get\_subject\_pkcs10, 60
- handlers, 61
- host, 61
- https\_server\_host, 62
- https\_server\_port, 62
- issue\_subject\_cert\_maybe, 60
- port, 62
- rootd\_bpki\_cert, 62
- rootd\_bpki\_crl, 62
- rootd\_bpki\_key, 62
- rpki\_base\_uri, 62
- rpki\_class\_name, 63
- rpki\_root\_cert, 63
- rpki\_root\_cert\_uri, 63
- rpki\_root\_crl, 63
- rpki\_root\_dir, 63
- rpki\_root\_key, 63
- rpki\_root\_manifest, 63
- rpki\_subject\_cert, 64
- rpki\_subject\_lifetime, 64
- rpki\_subject\_pkcs10, 64
- rpki\_subject\_regen, 64
- server\_cert, 64
- set\_subject\_cert, 60
- set\_subject\_pkcs10, 60
- up\_down\_handler, 60
- rootd.py(2481), 399
- rootd::cms\_msg, 118
- saxify, 118
- rootd::issue\_pdu, 118
- serve\_pdu, 119
- rootd::list\_pdu, 119
- serve\_pdu, 119
- rootd::message\_pdu, 120
- name2type, 120
- type2name, 120
- rootd::revoke\_pdu, 121
- serve\_pdu, 121
- rootd::sax\_handler, 121
- pdu, 122
- rootd\_bpki\_cert
- rootd, 62
- rootd\_bpki\_crl
- rootd, 62
- rootd\_bpki\_key
- rootd, 62
- route\_origins
- rpki::left\_right::self\_elt, 208
- rpki::rpki\_engine::ca\_detail\_obj,
- 272
- rpki, 65
- rpki.async, 65
- rpki.config, 67
- rpki.exceptions, 68
- rpki.https, 69
- rpki.ipaddrs, 73
- rpki.left\_right, 74
- rpki.log, 75
- rpki.manifest, 78
- rpki.oids, 79
- rpki.publication, 81
- rpki.relaxng, 82
- rpki.resource\_set, 83
- rpki.roa, 86
- rpki.rpki\_engine, 87
- rpki.sql, 88
- rpki.sundial, 89
- rpki.up\_down, 90
- rpki.x509, 92
- rpki.xml\_utils, 93
- rpki::async
- \_raiseExitNow, 66
- event\_loop, 66
- exit\_event\_loop, 66
- ExitNow, 67
- rpki::async::iterator, 122
- \_\_call\_\_, 123
- \_\_init\_\_, 123
- \_\_repr\_\_, 123
- caller\_function, 123
- done\_callback, 123
- ignore, 123
- item\_callback, 124
- iterator, 124
- rpki::async::timer, 124
- \_\_cmp\_\_, 125
- \_\_init\_\_, 125
- \_\_repr\_\_, 125

- cancel, 125
- clear, 126
- errback, 126, 128
- handler, 126, 128
- is\_set, 126
- queue, 128
- runq, 126
- seconds\_until\_wakeup, 127
- set, 127
- set\_errback, 127
- set\_handler, 127
- when, 128
- rpki::config::parser, 128
- \_\_init\_\_, 129
- default\_section, 130
- get, 129
- multiget, 129
- rpki::exceptions::BadClassNameSyntax, 130
- rpki::exceptions::BadClientURL, 130
- rpki::exceptions::BadContactURL, 130
- rpki::exceptions::BadExtension, 131
- rpki::exceptions::BadIRDBReply, 131
- rpki::exceptions::BadIssueResponse, 131
- rpki::exceptions::BadPKCS10, 132
- rpki::exceptions::BadPublicationReply, 132
- rpki::exceptions::BadQuery, 132
- rpki::exceptions::BadSender, 133
- rpki::exceptions::BadStatusCode, 133
- rpki::exceptions::BadURISyntax, 133
- rpki::exceptions::BSCNotFound, 134
- rpki::exceptions::ChildNotFound, 134
- rpki::exceptions::ClassNameMismatch, 134
- rpki::exceptions::ClassNameUnknown, 135
- rpki::exceptions::ClientNotFound, 135
- rpki::exceptions::CMSCRLNotSet, 135
- rpki::exceptions::CMSVerificationFailed, 136
- rpki::exceptions::DBConsistencyError, 136
- rpki::exceptions::DERObjectConversionError, 136
- rpki::exceptions::DuplicateObject, 137
- rpki::exceptions::EmptyPEM, 137
- rpki::exceptions::ForbiddenURI, 137
- rpki::exceptions::HTTPRequestFailed, 138
- rpki::exceptions::HTTPSClientAborted, 138
- rpki::exceptions::MissingCMSCRL, 138
- rpki::exceptions::MissingCMSEECert, 139
- rpki::exceptions::MultipleTLSEECert, 139
- rpki::exceptions::MustBePrefix, 139
- rpki::exceptions::NoActiveCA, 140
- rpki::exceptions::NotACertificateChain, 140
- rpki::exceptions::NotFound, 140
- rpki::exceptions::NotImplementedYet, 141
- rpki::exceptions::NotInDatabase, 141
- rpki::exceptions::ReceivedTLSCACert, 141
- rpki::exceptions::RPKI\_Exception, 142
- rpki::exceptions::ServerShuttingDown, 143
- rpki::exceptions::SKIMismatch, 143
- rpki::exceptions::SubprocessError, 143
- rpki::exceptions::TLSValidationError, 144
- rpki::exceptions::UnexpectedCMSCerts, 144
- rpki::exceptions::UnexpectedCMSCRLs, 144
- rpki::exceptions::UnparsableCMSDER, 145
- rpki::exceptions::UpstreamError, 145
- rpki::exceptions::WrongEContentType, 145
- rpki::https
  - build\_https\_ta\_cache, 71
  - client, 71
  - client\_queues, 72
  - debug, 72
  - debug\_tls\_certs, 72
  - default\_http\_version, 72
  - default\_timeout, 72
  - logger, 71

- rpki\_content\_type, 72
- server, 71
- want\_persistent\_client, 72
- want\_persistent\_server, 73
- rpki::https::http\_client, 146
  - \_\_init\_\_, 147
  - cert, 148
  - expect\_close, 148
  - handle\_close, 147
  - handle\_connect, 147
  - handle\_error, 147
  - handle\_message, 147
  - handle\_no\_content\_length, 147
  - handle\_timeout, 147
  - hostport, 148
  - key, 149
  - parse\_type, 149
  - queue, 149
  - retry\_read, 149
  - retry\_write, 149
  - send\_request, 148
  - set\_state, 148
  - start, 148
  - state, 149
  - ta, 149
  - tls, 150
  - tls\_connect, 148
- rpki::https::http\_listener, 150
  - \_\_init\_\_, 151
  - cert, 151
  - dynamic\_ta, 151
  - handle\_accept, 151
  - handle\_error, 151
  - handlers, 151
  - key, 151
  - log, 152
  - ta, 152
- rpki::https::http\_message, 152
  - \_\_init\_\_, 153
  - \_\_str\_\_, 153
  - body, 154
  - format, 153
  - headers, 154
  - normalize\_headers, 153
  - parse\_from\_wire, 153
  - parse\_version, 153
  - persistent, 153
  - software\_name, 154
  - version, 154
- rpki::https::http\_queue, 154
  - \_\_init\_\_, 155
  - cert, 156
  - client, 156
  - detach, 155
  - hostport, 156
  - key, 156
  - log, 156
  - queue, 157
  - request, 155
  - restart, 155
  - return\_result, 156
  - send\_request, 156
  - ta, 157
- rpki::https::http\_request, 157
  - \_\_init\_\_, 158
  - callback, 158
  - cmd, 158
  - errback, 158
  - format\_first\_line, 158
  - parse\_first\_line, 158
  - path, 158
  - retried, 159
- rpki::https::http\_response, 159
  - \_\_init\_\_, 159
  - code, 160
  - format\_first\_line, 159
  - parse\_first\_line, 160
  - reason, 160
- rpki::https::http\_server, 160
  - \_\_init\_\_, 161
  - expect\_close, 162
  - find\_handler, 161
  - handle\_message, 161
  - handle\_no\_content\_length, 161
  - handlers, 162
  - parse\_type, 162
  - retry\_read, 162
  - retry\_write, 163
  - send\_error, 161
  - send\_message, 162
  - send\_reply, 162
  - tls, 163

- tls\_accept, 162
- rpki::https::http\_stream, 163
  - \_\_init\_\_, 164
  - buffer, 168
  - chunk\_body, 164
  - chunk\_discard\_crlf, 165
  - chunk\_discard\_trailer, 165
  - chunk\_handler, 168
  - chunk\_header, 165
  - close, 165
  - collect\_incoming\_data, 165
  - found\_terminator, 165
  - get\_buffer, 165
  - handle\_body, 166
  - handle\_close, 166
  - handle\_error, 166
  - handle\_read, 166
  - handle\_timeout, 166
  - handle\_write, 166
  - initate\_send, 166
  - log, 168
  - log\_cert, 167
  - msg, 168
  - readable, 167
  - recv, 167
  - restart, 167
  - retry\_read, 168
  - retry\_write, 168
  - send, 167
  - timeout, 169
  - timer, 169
  - tls, 169
  - update\_timeout, 167
  - writeable, 167
- rpki::ipaddr::v4addr, 169
  - \_\_new\_\_, 170
  - \_\_str\_\_, 170
  - bits, 171
  - from\_bytes, 170
  - to\_bytes, 170
- rpki::ipaddr::v6addr, 171
  - \_\_new\_\_, 171
  - \_\_str\_\_, 171
  - bits, 172
  - from\_bytes, 172
  - to\_bytes, 172
- rpki::left\_right
  - enforce\_strict\_up\_down\_xml\_sender, 75
- rpki::left\_right::bsc\_elt, 172
  - attributes, 174
  - booleans, 174
  - children, 173
  - element\_name, 175
  - elements, 175
  - parents, 173
  - pkcs10\_request, 175
  - private\_key\_id, 175
  - repositories, 174
  - serve\_pre\_save\_hook, 174
  - signing\_cert, 175
  - signing\_cert\_crl, 175
  - sql\_template, 176
- rpki::left\_right::child\_elt, 176
  - attributes, 178
  - booleans, 179
  - bpki\_cert, 179
  - bpki\_glue, 179
  - ca\_from\_class\_name, 177
  - child\_certs, 177
  - clear\_https\_ta\_cache, 179
  - element\_name, 179
  - elements, 179
  - endElement, 177
  - parents, 178
  - serve\_post\_save\_hook, 178
  - serve\_up\_down, 178
  - sql\_template, 180
- rpki::left\_right::cms\_msg, 180
  - encoding, 180
  - saxify, 180
  - schema, 181
- rpki::left\_right::data\_elt, 181
  - bsc, 182
  - make\_reply\_clone\_hook, 182
  - self, 182
  - self\_id, 183
  - serve\_fetch\_all, 182
  - serve\_fetch\_one\_maybe, 182
  - serve\_pre\_save\_hook, 183
  - unimplemented\_control, 183



- rpki::left\_right::left\_right\_namespace,
  - 184
  - nsmmap, 184
  - xmlns, 184
- rpki::left\_right::list\_resources\_elt, 184
  - asn, 186
  - attributes, 186
  - element\_name, 186
  - ipv4, 186
  - ipv6, 186
  - startElement, 185
  - toXML, 185
  - valid\_until, 187
- rpki::left\_right::msg, 187
  - pdus, 188
  - serve\_top\_level, 188
  - version, 188
- rpki::left\_right::parent\_elt, 188
  - attributes, 191
  - booleans, 191
  - bpki\_cms\_cert, 191
  - bpki\_cms\_glue, 191
  - bpki\_https\_cert, 191
  - bpki\_https\_glue, 191
  - cas, 189
  - element\_name, 192
  - elements, 192
  - query\_up\_down, 189
  - repository, 190
  - serve\_post\_save\_hook, 190
  - serve\_rekey, 190
  - serve\_revoke, 190
  - sql\_template, 192
- rpki::left\_right::report\_error\_elt, 192
  - attributes, 193
  - element\_name, 194
  - error\_code, 194
  - from\_exception, 193
  - self\_handle, 194
  - text, 194
- rpki::left\_right::repository\_elt, 194
  - attributes, 196
  - bpki\_cms\_cert, 196
  - bpki\_cms\_glue, 196
  - bpki\_https\_cert, 196
  - bpki\_https\_glue, 197
  - call\_pubd, 195
  - element\_name, 197
  - elements, 197
  - parents, 195
  - publish, 195
  - sql\_template, 197
  - withdraw, 196
- rpki::left\_right::route\_origin\_elt, 198
  - as\_number, 202
  - attributes, 202
  - booleans, 203
  - ca\_detail, 199
  - ca\_detail\_id, 203
  - cert, 203
  - ee\_uri, 199
  - ee\_uri\_tail, 199
  - element\_name, 203
  - generate\_roa, 199
  - ipv4, 203
  - ipv6, 204
  - publish\_ee\_separately, 204
  - regenerate\_roa, 200
  - roa, 204
  - roa\_uri, 200
  - roa\_uri\_tail, 200
  - serve\_post\_save\_hook, 200
  - sql\_delete\_hook, 201
  - sql\_fetch\_hook, 201
  - sql\_insert\_hook, 201
  - sql\_template, 204
  - startElement, 201
  - update\_roa, 202
  - withdraw\_roa, 202
- rpki::left\_right::sax\_handler, 204
  - name, 205
  - pdu, 205
  - version, 205
- rpki::left\_right::self\_elt, 205
  - attributes, 210
  - booleans, 210
  - bpki\_cert, 211
  - bpki\_glue, 211
  - bscs, 207
  - children, 207
  - client\_poll, 207
  - crl\_interval, 211

- element\_name, 211
- elements, 211
- parents, 207
- regen\_margin, 211
- regenerate\_crls\_and\_manifests, 207
- repositories, 208
- route\_origins, 208
- self\_id, 212
- serve\_fetch\_all, 208
- serve\_fetch\_handle, 208
- serve\_fetch\_one\_maybe, 209
- serve\_post\_save\_hook, 209
- serve\_pre\_save\_hook, 209
- serve\_rekey, 209
- serve\_revoke, 210
- sql\_template, 212
- update\_children, 210
- update\_roas, 210
- use\_hsm, 212
- rpki::log
  - debug, 77
  - enable\_trace, 77
  - error, 77
  - info, 77
  - init, 76
  - note, 78
  - pid, 78
  - set\_trace, 77
  - tag, 78
  - trace, 77
  - use\_syslog, 78
  - warn, 78
- rpki::log::logger, 212
  - \_\_call\_\_, 213
  - \_\_init\_\_, 213
  - priority, 213
- rpki::manifest::FileAndHash, 213
  - \_\_init\_\_, 214
  - file, 214
  - hash, 214
- rpki::manifest::FilesAndHashes, 214
  - \_\_init\_\_, 215
- rpki::manifest::Manifest, 215
  - \_\_init\_\_, 216
  - explicitVersion, 216
  - fileHashAlg, 216
  - fileList, 216
  - manifestNumber, 216
  - nextUpdate, 216
  - thisUpdate, 216
  - version, 216
- rpki::oids
  - name2oid, 80
  - oid2name, 80
- rpki::publication
  - obj2elt, 82
- rpki::publication::certificate\_elt, 217
  - element\_name, 217
  - payload\_type, 217
- rpki::publication::client\_elt, 218
  - attributes, 220
  - base\_uri, 220
  - bpki\_cert, 220
  - bpki\_glue, 220
  - check\_allowed\_uri, 218
  - clear\_https\_ta\_cache, 220
  - element\_name, 220
  - elements, 220
  - endElement, 218
  - serve\_fetch\_all, 219
  - serve\_fetch\_one\_maybe, 219
  - serve\_post\_save\_hook, 219
  - sql\_template, 221
- rpki::publication::cms\_msg, 221
  - encoding, 222
  - saxify, 222
  - schema, 222
- rpki::publication::config\_elt, 222
  - attributes, 224
  - config\_id, 224
  - element\_name, 224
  - elements, 224
  - fetch, 223
  - serve\_fetch\_one\_maybe, 223
  - serve\_set, 223
  - sql\_template, 225
  - startElement, 224
  - wired\_in\_config\_id, 225
- rpki::publication::control\_elt, 225
  - serve\_dispatch, 226
- rpki::publication::crl\_elt, 226
  - element\_name, 226

- payload\_type, 226
- rpki::publication::manifest\_elt, 227
  - element\_name, 227
  - payload\_type, 227
- rpki::publication::msg, 228
  - pdu, 228
  - serve\_top\_level, 228
  - version, 229
- rpki::publication::publication\_namespace, 229
  - nsmap, 229
  - xmlns, 230
- rpki::publication::publication\_object\_elt, 230
  - attributes, 232
  - endElement, 231
  - payload, 232
  - serve\_dispatch, 231
  - serve\_publish, 231
  - serve\_withdraw, 231
  - toXML, 231
  - uri\_to\_filename, 232
- rpki::publication::report\_error\_elt, 232
  - attributes, 233
  - element\_name, 233
  - error\_code, 234
  - from\_exception, 233
- rpki::publication::roa\_elt, 234
  - element\_name, 234
  - payload\_type, 234
- rpki::publication::sax\_handler, 235
  - name, 235
  - pdu, 235
  - version, 235
- rpki::relaxng
  - left\_right, 82
  - publication, 83
  - up\_down, 83
- rpki::resource\_set
  - \_bs2long, 85
  - \_long2bs, 85
  - \_rsplit, 85
  - inherit\_token, 86
  - test1, 85
  - test2, 85
- rpki::resource\_set::resource\_bag, 236
  - \_\_eq\_\_, 237
  - \_\_init\_\_, 237
  - \_\_ne\_\_, 237
  - \_\_str\_\_, 237
  - asn, 238
  - empty, 237
  - from\_rfc3779\_tuples, 237
  - intersection, 237
  - oversized, 238
  - undersized, 238
  - union, 238
  - v4, 238
  - v6, 239
  - valid\_until, 239
- rpki::resource\_set::resource\_range, 239
  - \_\_cmp\_\_, 240
  - \_\_init\_\_, 240
  - max, 240
  - min, 240
- rpki::resource\_set::resource\_range\_as, 241
  - \_\_str\_\_, 241
  - datum\_type, 242
  - min, 242
  - to\_rfc3779\_tuple, 241
- rpki::resource\_set::resource\_range\_ip, 242
  - \_\_str\_\_, 243
  - \_prefixlen, 243
  - make\_prefix, 243
  - to\_rfc3779\_tuple, 243
- rpki::resource\_set::resource\_range\_ipv4, 244
  - datum\_type, 244
- rpki::resource\_set::resource\_range\_ipv6, 245
  - datum\_type, 245
- rpki::resource\_set::resource\_set, 245
  - \_\_init\_\_, 246
  - \_\_str\_\_, 246
  - \_comm, 246
  - contains, 247
  - difference, 247
  - from\_sql, 247
  - inherit, 249
  - intersection, 247

- issubset, 248
- issuperset, 248
- symmetric\_difference, 248
- union, 248
- rpki::resource\_set::resource\_set\_as, 249
  - inherit, 250
  - parse\_rfc3779\_tuple, 250
  - parse\_str, 250
  - range\_type, 250
  - to\_rfc3779\_tuple, 250
- rpki::resource\_set::resource\_set\_ip, 251
  - inherit, 252
  - parse\_rfc3779\_tuple, 251
  - parse\_str, 251
  - to\_rfc3779\_tuple, 252
- rpki::resource\_set::resource\_set\_ipv4, 252
  - afi, 253
  - range\_type, 253
- rpki::resource\_set::resource\_set\_ipv6, 253
  - afi, 254
  - range\_type, 254
- rpki::resource\_set::roa\_prefix, 254
  - \_\_cmp\_\_, 255
  - \_\_init\_\_, 255
  - \_\_str\_\_, 255
  - address, 257
  - max, 256
  - max\_prefixlen, 257
  - min, 256
  - prefixlen, 257
  - to\_resource\_range, 256
  - to\_roa\_tuple, 256
- rpki::resource\_set::roa\_prefix\_ipv4, 257
  - range\_type, 258
- rpki::resource\_set::roa\_prefix\_ipv6, 258
  - range\_type, 258
- rpki::resource\_set::roa\_prefix\_set, 259
  - \_\_init\_\_, 259
  - \_\_str\_\_, 259
  - from\_sql, 259
  - parse\_str, 260
  - to\_resource\_set, 260
  - to\_roa\_tuple, 260
- rpki::resource\_set::roa\_prefix\_set\_ipv4, 261
  - prefix\_type, 261
  - resource\_set\_type, 261
- rpki::resource\_set::roa\_prefix\_set\_ipv6, 262
  - prefix\_type, 262
  - resource\_set\_type, 262
- rpki::roa::ROAIPAddress, 263
  - \_\_init\_\_, 263
  - address, 263
  - maxLength, 263
- rpki::roa::ROAIPAddresses, 264
  - \_\_init\_\_, 264
- rpki::roa::ROAIPAddressFamilies, 264
  - \_\_init\_\_, 265
- rpki::roa::ROAIPAddressFamily, 265
  - \_\_init\_\_, 265
  - addresses, 266
  - addressFamily, 266
- rpki::roa::RouteOriginAttestation, 266
  - \_\_init\_\_, 266
  - asID, 267
  - explicitVersion, 267
  - ipAddrBlocks, 267
  - version, 267
- rpki::rpki\_engine::ca\_detail\_obj, 267
  - activate, 269
  - ca, 269
  - ca\_cert\_uri, 273
  - ca\_id, 273
  - child\_certs, 269
  - create, 269
  - crl\_uri, 269
  - crl\_uri\_tail, 269
  - delete, 270
  - gctx, 273
  - generate\_crl, 270
  - generate\_manifest, 270
  - generate\_manifest\_cert, 270
  - issue, 270
  - issue\_ee, 271
  - latest\_ca\_cert, 273
  - latest\_crl, 273
  - latest\_manifest, 273
  - latest\_manifest\_cert, 273

- manifest\_private\_key\_id, 273
- manifest\_public\_key, 274
- manifest\_uri, 271
- nextUpdate, 274
- private\_key\_id, 274
- public\_key, 274
- revoke, 271
- revoked\_certs, 272
- route\_origins, 272
- sql\_decode, 272
- sql\_template, 274
- state, 275
- update, 272
- rpki::rpki\_engine::ca\_obj, 275
  - ca\_details, 276
  - check\_for\_updates, 276
  - construct\_sia\_uri, 276
  - create, 276
  - delete, 277
  - fetch\_active, 277
  - fetch\_deprecated, 277
  - fetch\_pending, 277
  - fetch\_revoked, 277
  - gctx, 279
  - last\_crl\_sn, 279
  - last\_issued\_sn, 279
  - last\_manifest\_sn, 279
  - next\_crl\_number, 278
  - next\_manifest\_number, 278
  - next\_serial\_number, 278
  - parent, 278
  - parent\_id, 279
  - parent\_resource\_class, 280
  - rekey, 278
  - revoke, 279
  - sia\_uri, 280
  - sql\_template, 280
- rpki::rpki\_engine::child\_cert\_obj, 280
  - \_\_init\_\_, 281
  - ca\_detail, 281
  - ca\_detail\_id, 283
  - cert, 283
  - child, 281
  - child\_id, 283
  - fetch, 282
  - gctx, 283
  - reissue, 282
  - revoke, 282
  - sql\_template, 283
  - uri, 282
  - uri\_tail, 283
- rpki::rpki\_engine::revoked\_cert\_obj, 284
  - \_\_init\_\_, 285
  - ca\_detail, 285
  - ca\_detail\_id, 285
  - expires, 285
  - gctx, 286
  - revoke, 285
  - revoked, 286
  - serial, 286
  - sql\_template, 286
- rpki::rpki\_engine::rpkid\_context, 287
  - \_\_init\_\_, 288
  - bpki\_ta, 289
  - build\_https\_ta\_cache, 288
  - clear\_https\_ta\_cache, 288
  - cronjob\_handler, 288
  - https\_server\_host, 289
  - https\_server\_port, 289
  - https\_ta\_cache, 289
  - irbe\_cert, 289
  - irdb\_cert, 290
  - irdb\_query, 288
  - irdb\_url, 290
  - left\_right\_handler, 288
  - publication\_kludge\_base, 290
  - rpkid\_cert, 290
  - rpkid\_key, 290
  - sql, 290
  - up\_down\_handler, 289
  - up\_down\_url\_regexp, 290
- rpki::sql::session, 291
  - \_\_init\_\_, 292
  - \_exceptions\_enabled, 294
  - \_wrap\_execute, 292
  - assert\_pristine, 292
  - cache, 294
  - cache\_clear, 292
  - close, 292
  - connect, 293
  - cur, 294
  - database, 294

- db, 294
- dirty, 294
- execute, 293
- executemany, 293
- fetchall, 293
- lastrowid, 293
- password, 294
- ping, 293
- sweep, 293
- username, 295
- rpki::sql::sql\_persistent, 295
  - getx, 300
  - sql\_debug, 300
  - sql\_decode, 296
  - sql\_delete, 296
  - sql\_delete\_hook, 296
  - sql\_deleted, 300
  - sql\_encode, 297
  - sql\_fetch, 297
  - sql\_fetch\_all, 297
  - sql\_fetch\_hook, 297
  - sql\_fetch\_where, 298
  - sql\_fetch\_where1, 298
  - sql\_in\_db, 300
  - sql\_init, 298
  - sql\_insert\_hook, 298
  - sql\_is\_dirty, 298
  - sql\_mark\_clean, 299
  - sql\_mark\_deleted, 299
  - sql\_mark\_dirty, 299
  - sql\_store, 299
  - sql\_update\_hook, 299
- rpki::sql::template, 301
  - \_\_init\_\_, 301
  - columns, 301
  - delete, 301
  - index, 302
  - insert, 302
  - map, 302
  - select, 302
  - table, 302
  - update, 302
- rpki::sundial
  - now, 90
  - test, 90
- rpki::sundial::datetime, 303
  - \_\_add\_\_, 303
  - \_\_str\_\_, 304
  - \_\_sub\_\_, 304
  - earlier, 304
  - from\_sql, 304
  - fromASN1tuple, 304
  - fromdatetime, 304
  - fromGeneralizedTime, 305
  - fromUTCTime, 305
  - fromXMLtime, 305
  - later, 305
  - PKIX\_threshold, 307
  - to\_sql, 305
  - toASN1tuple, 306
  - toGeneralizedTime, 306
  - totimestamp, 306
  - toUTCTime, 306
  - toXMLtime, 306
- rpki::sundial::timedelta, 307
  - convert\_to\_seconds, 308
  - fromtimedelta, 308
  - parse, 308
  - regex, 308
- rpki::up\_down
  - nsmmap, 91
  - xmlns, 91
- rpki::up\_down::base\_elt, 309
  - check\_response, 310
  - endElement, 310
  - make\_b64elt, 310
  - make\_elt, 310
  - serve\_pdu, 310
  - startElement, 311
- rpki::up\_down::certificate\_elt, 311
  - cert, 313
  - cert\_url, 313
  - endElement, 312
  - req\_resource\_set\_as, 313
  - req\_resource\_set\_ipv4, 313
  - req\_resource\_set\_ipv6, 313
  - startElement, 312
  - toXML, 312
- rpki::up\_down::class\_elt, 313
  - \_\_init\_\_, 314
  - cert\_url, 315
  - certs, 315

- class\_name, 316
- endElement, 314
- from\_resource\_bag, 315
- issuer, 316
- resource\_set\_as, 316
- resource\_set\_ipv4, 316
- resource\_set\_ipv6, 316
- resource\_set\_notafter, 316
- startElement, 315
- suggested\_sia\_head, 316
- to\_resource\_bag, 315
- toXML, 315
- rpki::up\_down::class\_response\_syntax, 317
  - \_\_init\_\_, 317
  - classes, 318
  - startElement, 317
  - toXML, 318
- rpki::up\_down::cms\_msg, 318
  - encoding, 319
  - saxify, 319
  - schema, 319
- rpki::up\_down::error\_response\_pdu, 319
  - \_\_init\_\_, 320
  - check\_response, 320
  - codes, 321
  - description, 321
  - endElement, 320
  - exceptions, 321
  - status, 322
  - toXML, 321
- rpki::up\_down::issue\_pdu, 322
  - class\_name, 324
  - endElement, 323
  - pkcs10, 324
  - query, 323
  - req\_resource\_set\_as, 324
  - req\_resource\_set\_ipv4, 324
  - req\_resource\_set\_ipv6, 324
  - serve\_pdu, 323
  - startElement, 323
  - toXML, 323
- rpki::up\_down::issue\_response\_pdu, 325
  - check\_response, 325
- rpki::up\_down::list\_pdu, 325
  - query, 326
  - serve\_pdu, 326
  - toXML, 326
- rpki::up\_down::list\_response\_pdu, 326
- rpki::up\_down::message\_pdu, 327
  - \_\_str\_\_, 328
  - make\_query, 328
  - name2type, 329
  - payload, 329
  - recipient, 329
  - sender, 330
  - serve\_error, 328
  - serve\_top\_level, 328
  - startElement, 328
  - toXML, 329
  - type, 330
  - type2name, 330
  - version, 330
- rpki::up\_down::multi\_uri, 330
  - \_\_init\_\_, 331
  - \_\_str\_\_, 331
  - rsync, 331
- rpki::up\_down::revoke\_pdu, 332
  - class\_name, 333
  - get\_SKI, 332
  - query, 332
  - serve\_pdu, 332
  - ski, 333
- rpki::up\_down::revoke\_response\_pdu, 333
- rpki::up\_down::revoke\_syntax, 334
  - class\_name, 335
  - ski, 335
  - startElement, 334
  - toXML, 334
- rpki::up\_down::sax\_handler, 335
  - name, 335
  - pdu, 336
  - version, 336
- rpki::x509
  - calculate\_SKI, 93
  - POWify\_OID, 93
- rpki::x509::CMS\_object, 336
  - content, 339
  - debug\_cms\_certs, 339
  - DER, 339
  - dump\_on\_verify\_failure, 339

- econtent\_oid, 340
- extract, 337
- formats, 340
- get\_content, 338
- get\_DER, 338
- get\_POW, 338
- other\_clear, 340
- pem\_converter, 340
- POW, 341
- print\_on\_der\_error, 341
- require\_crls, 341
- set\_content, 338
- sign, 338
- verify, 339
- rpki::x509::CRL, 341
  - DER, 344
  - formats, 344
  - generate, 342
  - get\_DER, 342
  - get\_POW, 342
  - get\_POWpkix, 343
  - getIssuer, 343
  - getNextUpdate, 343
  - getThisUpdate, 343
  - pem\_converter, 344
  - POW, 344
  - POWpkix, 344
- rpki::x509::DER\_CMS\_object, 345
  - content, 346
  - decode, 345
  - encode, 345
- rpki::x509::DER\_object, 346
  - \_\_cmp\_\_, 347
  - \_\_init\_\_, 347
  - clear, 347
  - DER, 352
  - dumpasn1, 348
  - empty, 348
  - formats, 352
  - from\_sql, 348
  - gAKI, 348
  - get\_3779resources, 348
  - get\_AIA, 349
  - get\_AKI, 349
  - get\_Base64, 349
  - get\_basicConstraints, 349
  - get\_DER, 349
  - get\_PEM, 350
  - get\_SIA, 350
  - get\_SKI, 350
  - gSKI, 350
  - hAKI, 351
  - hSKI, 351
  - is\_CA, 351
  - other\_clear, 352
  - pem\_converter, 352
  - set, 351
  - to\_sql, 352
- rpki::x509::PEM\_converter, 353
  - \_\_init\_\_, 353
  - b, 354
  - e, 354
  - looks\_like\_PEM, 353
  - to\_DER, 354
  - to\_PEM, 354
- rpki::x509::PKCS10, 355
  - check\_valid\_rpki, 355
  - create, 356
  - create\_ca, 356
  - DER, 357
  - formats, 357
  - get\_DER, 356
  - get\_POWpkix, 356
  - getPublicKey, 356
  - pem\_converter, 357
  - POWpkix, 357
- rpki::x509::ROA, 358
  - build, 358
  - content\_class, 358
  - econtent\_oid, 358
  - pem\_converter, 359
- rpki::x509::RSA, 359
  - DER, 361
  - formats, 361
  - generate, 360
  - get\_DER, 360
  - get\_POW, 360
  - get\_public\_DER, 360
  - get\_RSAPublic, 361
  - get\_SKI, 361
  - get\_tlslite, 361
  - pem\_converter, 362



- POW, 362
- tlslite, 362
- rpki::x509::RSAPublic, 362
  - DER, 364
  - formats, 364
  - get\_DER, 363
  - get\_POW, 363
  - get\_SKI, 363
  - pem\_converter, 364
  - POW, 364
- rpki::x509::SignedManifest, 365
  - build, 365
  - content\_class, 366
  - content\_oid, 366
  - getNextUpdate, 365
  - getThisUpdate, 366
  - pem\_converter, 366
- rpki::x509::X509, 367
  - DER, 370
  - expired, 368
  - formats, 371
  - get\_DER, 368
  - get\_POW, 368
  - get\_POWpkix, 368
  - get\_tlslite, 368
  - getIssuer, 369
  - getNotAfter, 369
  - getNotBefore, 369
  - getPublicKey, 369
  - getSerial, 369
  - getSubject, 370
  - issue, 370
  - normalize\_chain, 370
  - pem\_converter, 371
  - POW, 371
  - POWpkix, 371
  - tlslite, 371
- rpki::x509::XML\_CMS\_object, 372
  - content, 374
  - decode, 372
  - dump\_inbound\_cms, 374
  - dump\_outbound\_cms, 374
  - dump\_to\_disk, 372
  - content\_oid, 374
  - encode, 373
  - pretty\_print\_content, 373
  - schema\_check, 373
  - unwrap, 373
  - wrap, 373
- rpki::xml\_utils::base\_elt, 375
  - \_\_str\_\_, 376
  - attributes, 377
  - booleans, 377
  - elements, 378
  - endElement, 376
  - make\_b64elt, 376
  - make\_elt, 376
  - make\_pdu, 376
  - read\_attrs, 376
  - startElement, 377
  - toXML, 377
- rpki::xml\_utils::data\_elt, 378
  - endElement, 379
  - make\_reply, 379
  - make\_reply\_clone\_hook, 379
  - serve\_create, 379
  - serve\_destroy, 380
  - serve\_dispatch, 380
  - serve\_fetch\_one, 380
  - serve\_get, 380
  - serve\_list, 380
  - serve\_post\_save\_hook, 381
  - serve\_pre\_save\_hook, 381
  - serve\_set, 381
  - toXML, 381
  - unimplemented\_control, 382
- rpki::xml\_utils::msg, 382
  - \_\_str\_\_, 383
  - endElement, 383
  - startElement, 383
  - toXML, 383
  - type, 384
  - version, 384
- rpki::xml\_utils::sax\_handler, 384
  - \_\_init\_\_, 385
  - characters, 385
  - create\_top\_level, 385
  - endElement, 385
  - endElementNS, 386
  - result, 387
  - saxify, 386
  - stack, 387

- startElement, 386
- startElementNS, 386
- text, 387
- rpki\_base\_uri
  - rootd, 62
- rpki\_class\_name
  - rootd, 63
- rpki\_content\_type
  - rpki::https, 72
- rpki\_engine.py(2481), 401
- rpki\_root\_cert
  - rootd, 63
- rpki\_root\_cert\_uri
  - rootd, 63
- rpki\_root\_crl
  - rootd, 63
- rpki\_root\_dir
  - rootd, 63
- rpki\_root\_key
  - rootd, 63
- rpki\_root\_manifest
  - rootd, 63
- rpki\_subject\_cert
  - rootd, 64
- rpki\_subject\_lifetime
  - rootd, 64
- rpki\_subject\_pkcs10
  - rootd, 64
- rpki\_subject\_regen
  - rootd, 64
- rpkid, 94
  - cfg\_file, 95
  - main, 95
  - profile, 95
- rpkid.py(2452), 401
- rpkid\_cert
  - irdbd, 55
  - rpki::rpki\_engine::rpkid\_context, 290
- rpkid\_key
  - rpki::rpki\_engine::rpkid\_context, 290
- rsync
  - rpki::up\_down::multi\_uri, 331
- runq
  - rpki::async::timer, 126
- saxify
  - irbe\_cli::left\_right\_cms\_msg, 106
  - irbe\_cli::publication\_cms\_msg, 108
  - rootd::cms\_msg, 118
  - rpki::left\_right::cms\_msg, 180
  - rpki::publication::cms\_msg, 222
  - rpki::up\_down::cms\_msg, 319
  - rpki::xml\_utils::sax\_handler, 386
- schema
  - rpki::left\_right::cms\_msg, 181
  - rpki::publication::cms\_msg, 222
  - rpki::up\_down::cms\_msg, 319
- schema\_check
  - rpki::x509::XML\_CMS\_object, 373
- seconds\_until\_wakeup
  - rpki::async::timer, 127
- select
  - rpki::sql::template, 302
- self
  - rpki::left\_right::data\_elt, 182
- self\_handle
  - rpki::left\_right::report\_error\_elt, 194
- self\_id
  - rpki::left\_right::data\_elt, 183
  - rpki::left\_right::self\_elt, 212
- send
  - rpki::https::http\_stream, 167
- send\_error
  - rpki::https::http\_server, 161
- 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, 330
- Sequence, 387
- SequenceOf, 388
- serial
  - cross\_certify, 47
  - rpki::rpki\_engine::revoked\_cert\_obj, 286
- serial\_file
  - cross\_certify, 47

- serve\_create
  - rpki::xml\_utils::data\_elt, 379
- serve\_destroy
  - rpki::xml\_utils::data\_elt, 380
- serve\_dispatch
  - rpki::publication::control\_elt, 226
  - rpki::publication::publication\_  
object\_elt, 231
  - rpki::xml\_utils::data\_elt, 380
- serve\_error
  - rpki::up\_down::message\_pdu, 328
- serve\_fetch\_all
  - rpki::left\_right::data\_elt, 182
  - rpki::left\_right::self\_elt, 208
  - rpki::publication::client\_elt, 219
- serve\_fetch\_handle
  - rpki::left\_right::self\_elt, 208
- serve\_fetch\_one
  - rpki::xml\_utils::data\_elt, 380
- serve\_fetch\_one\_maybe
  - rpki::left\_right::data\_elt, 182
  - rpki::left\_right::self\_elt, 209
  - rpki::publication::client\_elt, 219
  - rpki::publication::config\_elt, 223
- serve\_get
  - rpki::xml\_utils::data\_elt, 380
- serve\_list
  - rpki::xml\_utils::data\_elt, 380
- serve\_pdu
  - rootd::issue\_pdu, 119
  - rootd::list\_pdu, 119
  - rootd::revoke\_pdu, 121
  - rpki::up\_down::base\_elt, 310
  - rpki::up\_down::issue\_pdu, 323
  - rpki::up\_down::list\_pdu, 326
  - rpki::up\_down::revoke\_pdu, 332
- serve\_post\_save\_hook
  - rpki::left\_right::child\_elt, 178
  - rpki::left\_right::parent\_elt, 190
  - rpki::left\_right::route\_origin\_elt,  
200
  - rpki::left\_right::self\_elt, 209
  - rpki::publication::client\_elt, 219
  - rpki::xml\_utils::data\_elt, 381
- serve\_pre\_save\_hook
  - rpki::left\_right::bsc\_elt, 174
  - rpki::left\_right::data\_elt, 183
  - rpki::left\_right::self\_elt, 209
  - rpki::xml\_utils::data\_elt, 381
- serve\_publish
  - rpki::publication::publication\_  
object\_elt, 231
- serve\_rekey
  - rpki::left\_right::parent\_elt, 190
  - rpki::left\_right::self\_elt, 209
- serve\_revoke
  - rpki::left\_right::parent\_elt, 190
  - rpki::left\_right::self\_elt, 210
- serve\_set
  - rpki::publication::config\_elt, 223
  - rpki::xml\_utils::data\_elt, 381
- serve\_top\_level
  - rpki::left\_right::msg, 188
  - rpki::publication::msg, 228
  - rpki::up\_down::message\_pdu, 328
- serve\_up\_down
  - rpki::left\_right::child\_elt, 178
- serve\_withdraw
  - rpki::publication::publication\_  
object\_elt, 231
- server
  - rpki::https, 71
- server\_cert
  - irdbd, 55
  - rootd, 64
- server\_ta
  - irbe\_cli, 51
- set
  - rpki::async::timer, 127
  - rpki::x509::DER\_object, 351
- set\_content
  - rpki::x509::CMS\_object, 338
- set\_errback
  - rpki::async::timer, 127
- set\_handler
  - rpki::async::timer, 127
- set\_state
  - rpki::https::http\_client, 148
- set\_subject\_cert
  - rootd, 60
- set\_subject\_pkcs10
  - rootd, 60

- set\_trace
  - rpki::log, 77
- sia\_uri
  - rpki::rpki\_engine::ca\_obj, 280
- sign
  - rpki::x509::CMS\_object, 338
- signing\_cert
  - irbe\_cli::bsc\_elt, 98
  - rpki::left\_right::bsc\_elt, 175
- signing\_cert\_crl
  - irbe\_cli::bsc\_elt, 98
  - rpki::left\_right::bsc\_elt, 175
- ski
  - rpki::up\_down::revoke\_pdu, 333
  - rpki::up\_down::revoke\_syntax, 335
- software\_name
  - rpki::https::http\_message, 154
- sql
  - pubd::pubd\_context, 117
  - rpki::rpki\_engine::rpkid\_context, 290
- sql.py(2452), 401
- sql\_debug
  - rpki::sql::sql\_persistent, 300
- sql\_decode
  - rpki::rpki\_engine::ca\_detail\_obj, 272
  - rpki::sql::sql\_persistent, 296
- sql\_delete
  - rpki::sql::sql\_persistent, 296
- sql\_delete\_hook
  - rpki::left\_right::route\_origin\_elt, 201
  - rpki::sql::sql\_persistent, 296
- sql\_deleted
  - rpki::sql::sql\_persistent, 300
- sql\_encode
  - rpki::sql::sql\_persistent, 297
- sql\_fetch
  - rpki::sql::sql\_persistent, 297
- sql\_fetch\_all
  - rpki::sql::sql\_persistent, 297
- sql\_fetch\_hook
  - rpki::left\_right::route\_origin\_elt, 201
  - rpki::sql::sql\_persistent, 297
- sql\_fetch\_where
  - rpki::sql::sql\_persistent, 298
- sql\_fetch\_where1
  - rpki::sql::sql\_persistent, 298
- sql\_in\_db
  - rpki::sql::sql\_persistent, 300
- sql\_init
  - rpki::sql::sql\_persistent, 298
- sql\_insert\_hook
  - rpki::left\_right::route\_origin\_elt, 201
  - rpki::sql::sql\_persistent, 298
- sql\_is\_dirty
  - rpki::sql::sql\_persistent, 298
- sql\_mark\_clean
  - rpki::sql::sql\_persistent, 299
- sql\_mark\_deleted
  - rpki::sql::sql\_persistent, 299
- sql\_mark\_dirty
  - rpki::sql::sql\_persistent, 299
- sql\_store
  - rpki::sql::sql\_persistent, 299
- sql\_template
  - rpki::left\_right::bsc\_elt, 176
  - rpki::left\_right::child\_elt, 180
  - rpki::left\_right::parent\_elt, 192
  - rpki::left\_right::repository\_elt, 197
  - rpki::left\_right::route\_origin\_elt, 204
  - rpki::left\_right::self\_elt, 212
  - rpki::publication::client\_elt, 221
  - rpki::publication::config\_elt, 225
  - rpki::rpki\_engine::ca\_detail\_obj, 274
  - rpki::rpki\_engine::ca\_obj, 280
  - rpki::rpki\_engine::child\_cert\_obj, 283
  - rpki::rpki\_engine::revoked\_cert\_obj, 286
- sql\_update\_hook
  - rpki::sql::sql\_persistent, 299
- stack
  - rpki::xml\_utils::sax\_handler, 387
- start
  - rpki::https::http\_client, 148
- startElement

- rpki::left\_right::list\_resources\_elt, 185
- rpki::left\_right::route\_origin\_elt, 201
- rpki::publication::config\_elt, 224
- rpki::up\_down::base\_elt, 311
- rpki::up\_down::certificate\_elt, 312
- rpki::up\_down::class\_elt, 315
- rpki::up\_down::class\_response\_syntax, 317
- rpki::up\_down::issue\_pdu, 323
- rpki::up\_down::message\_pdu, 328
- rpki::up\_down::revoke\_syntax, 334
- rpki::xml\_utils::base\_elt, 377
- rpki::xml\_utils::msg, 383
- rpki::xml\_utils::sax\_handler, 386
- startElementNS
  - rpki::xml\_utils::sax\_handler, 386
- startup\_msg
  - irdbd, 56
- state
  - rpki::https::http\_client, 149
  - rpki::rpki\_engine::ca\_detail\_obj, 275
- status
  - rpki::up\_down::error\_response\_pdu, 322
- suggested\_sia\_head
  - rpki::up\_down::class\_elt, 316
- sundial.py(2452), 402
- sweep
  - rpki::sql::session, 293
- symmetric\_difference
  - rpki::resource\_set::resource\_set, 248
- ta
  - rpki::https::http\_client, 149
  - rpki::https::http\_listener, 152
  - rpki::https::http\_queue, 157
- table
  - rpki::sql::template, 302
- tag
  - rpki::log, 78
- test
  - rpki::sundial, 90
- test1
  - rpki::resource\_set, 85
- test2
  - rpki::resource\_set, 85
- text
  - rpki::left\_right::report\_error\_elt, 194
  - rpki::xml\_utils::sax\_handler, 387
- textwrap::TextWrapper, 388
- thisUpdate
  - rpki::manifest::Manifest, 216
- timeout
  - rpki::https::http\_stream, 169
- timer
  - rpki::https::http\_stream, 169
- tls
  - rpki::https::http\_client, 150
  - rpki::https::http\_server, 163
  - rpki::https::http\_stream, 169
- tls\_accept
  - rpki::https::http\_server, 162
- tls\_connect
  - rpki::https::http\_client, 148
- tlslite
  - rpki::x509::RSA, 362
  - rpki::x509::X509, 371
- to\_bytes
  - rpki::ipaddr::v4addr, 170
  - rpki::ipaddr::v6addr, 172
- to\_DER
  - rpki::x509::PEM\_converter, 354
- to\_PEM
  - rpki::x509::PEM\_converter, 354
- to\_resource\_bag
  - rpki::up\_down::class\_elt, 315
- to\_resource\_range
  - rpki::resource\_set::roa\_prefix, 256
- to\_resource\_set
  - rpki::resource\_set::roa\_prefix\_set, 260
- to\_rfc3779\_tuple
  - rpki::resource\_set::resource\_range\_as, 241
  - rpki::resource\_set::resource\_range\_ip, 243
  - rpki::resource\_set::resource\_set\_as, 250

- rpki::resource\_set::resource\_set\_ip, 252
- to\_roa\_tuple
  - rpki::resource\_set::roa\_prefix, 256
  - rpki::resource\_set::roa\_prefix\_set, 260
- to\_sql
  - rpki::sundial::datetime, 305
  - rpki::x509::DER\_object, 352
- toASN1tuple
  - rpki::sundial::datetime, 306
- toGeneralizedTime
  - rpki::sundial::datetime, 306
- top\_opts
  - irbe\_cli, 52
- totimestamp
  - rpki::sundial::datetime, 306
- toUTCTime
  - rpki::sundial::datetime, 306
- toXML
  - rpki::left\_right::list\_resources\_elt, 185
  - rpki::publication::publication\_object\_elt, 231
  - rpki::up\_down::certificate\_elt, 312
  - rpki::up\_down::class\_elt, 315
  - rpki::up\_down::class\_response\_syntax, 318
  - rpki::up\_down::error\_response\_pdu, 321
  - rpki::up\_down::issue\_pdu, 323
  - rpki::up\_down::list\_pdu, 326
  - rpki::up\_down::message\_pdu, 329
  - rpki::up\_down::revoke\_syntax, 334
  - rpki::xml\_utils::base\_elt, 377
  - rpki::xml\_utils::data\_elt, 381
  - rpki::xml\_utils::msg, 383
- toXMLtime
  - rpki::sundial::datetime, 306
- trace
  - rpki::log, 77
- type
  - rpki::up\_down::message\_pdu, 330
  - rpki::xml\_utils::msg, 384
- type2name
  - rootd::message\_pdu, 120
  - rpki::up\_down::message\_pdu, 330
- u
  - irdbd, 56
- undersized
  - rpki::resource\_set::resource\_bag, 238
- unimplemented\_control
  - rpki::left\_right::data\_elt, 183
  - rpki::xml\_utils::data\_elt, 382
- union
  - rpki::resource\_set::resource\_bag, 238
  - rpki::resource\_set::resource\_set, 248
- unwrap
  - rpki::x509::XML\_CMS\_object, 373
- up\_down
  - rpki::relaxng, 83
- up\_down.py(2481), 402
- up\_down\_handler
  - rootd, 60
  - rpki::rpki\_engine::rpkid\_context, 289
- up\_down\_url\_regexp
  - rpki::rpki\_engine::rpkid\_context, 290
- update
  - rpki::rpki\_engine::ca\_detail\_obj, 272
  - rpki::sql::template, 302
- update\_children
  - rpki::left\_right::self\_elt, 210
- update\_roa
  - rpki::left\_right::route\_origin\_elt, 202
- update\_roas
  - rpki::left\_right::self\_elt, 210
- update\_timeout
  - rpki::https::http\_stream, 167
- uri
  - rpki::rpki\_engine::child\_cert\_obj, 282
- uri\_tail
  - rpki::rpki\_engine::child\_cert\_obj, 283
- uri\_to\_filename

- rpki::publication::publication\_  
object\_elt, 232
- 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, 212
- use\_syslog
  - rpki::log, 78
- username
  - rpki::sql::session, 295
- v4
  - rpki::resource\_set::resource\_bag, 238
- v6
  - rpki::resource\_set::resource\_bag, 239
- valid\_until
  - rpki::left\_right::list\_resources\_elt, 187
  - rpki::resource\_set::resource\_bag, 239
- value
  - cross\_certify, 47
- verbose
  - irbe\_cli, 52
- verify
  - rpki::x509::CMS\_object, 339
- version
  - rpki::https::http\_message, 154
  - rpki::left\_right::msg, 188
  - rpki::left\_right::sax\_handler, 205
  - rpki::manifest::Manifest, 216
  - rpki::publication::msg, 229
  - rpki::publication::sax\_handler, 235
  - rpki::roa::RouteOriginAttestation, 267
  - rpki::up\_down::message\_pdu, 330
  - rpki::up\_down::sax\_handler, 336
  - rpki::xml\_utils::msg, 384
- want\_persistent\_client
  - rpki::https, 72
- want\_persistent\_server
  - rpki::https, 73
- warn
  - rpki::log, 78
- when
  - rpki::async::timer, 128
- wired\_in\_config\_id
  - rpki::publication::config\_elt, 225
- withdraw
  - rpki::left\_right::repository\_elt, 196
- withdraw\_roa
  - rpki::left\_right::route\_origin\_elt, 202
- wrap
  - rpki::x509::XML\_CMS\_object, 373
- writable
  - rpki::https::http\_stream, 167
- x
  - cross\_certify, 47
- x509.py(2481), 403
- xml::sax::handler::ContentHandler, 388
- xml\_utils.py(2452), 403
- xmlns
  - rpki::left\_right::left\_right\_  
namespace, 184
  - rpki::publication::publication\_  
namespace, 230
  - rpki::up\_down, 91