RPKI Engine

1.0

Generated by Doxygen 1.6.1

Tue Jan 12 02:46:40 2010

Contents

1 RPKI Engine Reference Manual 1

2 Further Reading 1

3 Installation Guide 2

4 Operation Guide 5

4.1 rpkid.py . . . 6

4.2 pubd.py . . . 7

4.3 rootd.py . . . 8

4.4 irdbd.py . . . 10

4.5 irbe_cli.py . . . 11

4.6 cross_certify.py . . . 13

4.7 irbe-setup.py con g le . . . 13

4.8 cronjob.py . . . 14

4.9 testbed.py: . . . 15

4.10 testpoke.py . . . 17

5 Left-right protocol 18

5.1 Terminology . . . 18

5.2 initiated by the IRBE . . . 19

5.2.1 <self/> object . . . 19

5.2.2 <bsc/> object . . . 21

5.2.3 <parent/> object . . . 22

5.2.4 <child/> object . . . 23

5.2.5 <repository/> object . . . 24

5.2.6 <route_origin/> object . . . 25

5.3 Operations initiated by the RPKI engine . . . 26

5.3.1 <list_resources/> messages . . . 26

5.4 Error handling . . . 27

6 Publication protocol 28

6.1 Terminology . . . 28
6.2 Publication control subprotocol . . . 28
6.2.1 <con g/> object . . . 29
6.2.2 <client/> object . . . 29
6.3 Publication subprotocol . . . 30
6.3.1 <certi cate/> object . . . 30
6.3.2 <crl/> object . . . 30
6.3.3 <manifest/> object . . . 30
6.3.4 <roa/> object . . . 30
6.4 Error handling . . . 30
6.5 Additional access control considerations . . . 31

7 SQL database schemas 32
7.1 rpkid SQL schema . . . 34
7.2 pubd SQL Schema . . . 38
7.3 irdbd SQL Schema . . . 40

8 BPKI model 42

9 Namespace Documentation 45
9.1 Package irbe_cli . . . 45
9.1.1 Detailed Description . . . 46
9.1.2 Function Documentation . . . 46
9.1.3 Variable Documentation . . . 47
9.2 Package irdbd . . . 49
9.2.1 Detailed Description . . . 49
9.2.2 Function Documentation . . . 50
9.2.3 Variable Documentation . . . 51
9.3 Package pubd . . . 53
9.3.1 Detailed Description . . . 53
9.3.2 Function Documentation . . . 54
9.3.3 Variable Documentation . . . 54

9.4 Package rootd . . . 55
9.4.1 Detailed Description . . . 56
9.4.2 Function Documentation . . . 57
9.4.3 Variable Documentation . . . 58
9.5 Package rpki . . . 62
9.6 Package rpki.async . . . 63
9.6.1 Detailed Description . . . 63
9.6.2 Function Documentation . . . 64
9.6.3 Variable Documentation . . . 65
9.7 Package rpki.config . . . 65
9.7.1 Detailed Description . . . 65
9.8 Package rpki.exceptions . . . 66
9.8.1 Detailed Description . . . 67
9.9 Package rpki.https . . . 68
9.9.1 Detailed Description . . . 69
9.9.2 Function Documentation . . . 69
9.9.3 Variable Documentation . . . 70
9.10 Package rpki.ipaddrs . . . 72
9.10.1 Detailed Description . . . 72
9.11 Package rpki.left_right . . . 73
9.11.1 Detailed Description . . . 73
9.11.2 Variable Documentation . . . 74
9.12 Package rpki.log . . . 74
9.12.1 Detailed Description . . . 75
9.12.2 Function Documentation . . . 75
9.12.3 Variable Documentation . . . 76
9.13 Package rpki.manifest . . . 77
9.13.1 Detailed Description . . . 77
9.14 Package rpki.oids . . . 78
9.14.1 Detailed Description . . . 78
9.14.2 Variable Documentation . . . 79

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

10 Class Documentation 95

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

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

10.24.1 Detailed Description . . . 112
10.25 irbe_cli.roa_elt Class Reference . . . 112
10.25.1 Detailed Description . . . 113
10.26 irbe_cli.self_elt Class Reference . . . 113
10.26.1 Detailed Description . . . 113
10.27 irbe_cli.UsageWrapper Class Reference . . . 113
10.27.1 Detailed Description . . . 113
10.27.2 Member Function Documentation . . . 113
10.28 long Class Reference . . . 114
10.29 object Class Reference . . . 114
10.30 pubd.pubd_context Class Reference . . . 114
10.30.1 Detailed Description . . . 115
10.30.2 Member Function Documentation . . . 115
10.30.3 Member Data Documentation . . . 116
10.31 datetime Class Reference . . . 118
10.32 timedelta Class Reference . . . 118
10.33 rootd.cms_msg Class Reference . . . 118
10.33.1 Detailed Description . . . 118
10.33.2 Member Data Documentation . . . 119
10.34 rootd.issue_pdu Class Reference . . . 119
10.34.1 Detailed Description . . . 119
10.34.2 Member Function Documentation . . . 119
10.35 rootd.list_pdu Class Reference . . . 119
10.35.1 Detailed Description . . . 120
10.35.2 Member Function Documentation . . . 120
10.36 rootd.message_pdu Class Reference . . . 120
10.36.1 Detailed Description . . . 120
10.36.2 Member Function Documentation . . . 121
10.36.3 Member Data Documentation . . . 121
10.37 rootd.revoke_pdu Class Reference . . . 121
10.37.1 Detailed Description . . . 122

10.37.2 Member Function Documentation 122
10.38 rootd.sax_handler Class Reference 122
10.38.1 Detailed Description 122
10.38.2 Member Data Documentation 122
10.39 rpki.async.gc_summary Class Reference 123
10.39.1 Detailed Description 123
10.39.2 Member Function Documentation 123
10.39.3 Member Data Documentation 124
10.40 rpki.async.iterator Class Reference 124
10.40.1 Detailed Description 124
10.40.2 Member Function Documentation 125
10.40.3 Member Data Documentation 126
10.41 rpki.async.sync_wrapper Class Reference 126
10.41.1 Detailed Description 127
10.41.2 Member Function Documentation 127
10.41.3 Member Data Documentation 128
10.42 rpki.async.timer Class Reference 128
10.42.1 Detailed Description 129
10.42.2 Member Function Documentation 130
10.42.3 Member Data Documentation 132
10.43 rpki.con g.parser Class Reference 133
10.43.1 Detailed Description 134
10.43.2 Member Function Documentation 134
10.43.3 Member Data Documentation 136
10.44 rpki.exceptions.BadClassNameSyntax Class Reference 137
10.44.1 Detailed Description 137
10.45 rpki.exceptions.BadClientURL Class Reference 137
10.45.1 Detailed Description 137
10.46 rpki.exceptions.BadContactURL Class Reference 137
10.46.1 Detailed Description 138
10.47 rpki.exceptions.BadExtension Class Reference 138

10.47.1 Detailed Description 138
10.48 rpki.exceptions.BadIRDBReply Class Reference 138
10.48.1 Detailed Description 138
10.49 rpki.exceptions.BadIssueResponse Class Reference 138
10.49.1 Detailed Description 139
10.50 rpki.exceptions.BadPKCS10 Class Reference 139
10.50.1 Detailed Description 139
10.51 rpki.exceptions.BadPublicationReply Class Reference 139
10.51.1 Detailed Description 139
10.52 rpki.exceptions.BadQuery Class Reference 139
10.52.1 Detailed Description 140
10.53 rpki.exceptions.BadSender Class Reference 140
10.53.1 Detailed Description 140
10.54 rpki.exceptions.BadStatusCode Class Reference 140
10.54.1 Detailed Description 140
10.55 rpki.exceptions.BadURISyntax Class Reference 140
10.55.1 Detailed Description 141
10.56 rpki.exceptions.BSCNotFound Class Reference 141
10.56.1 Detailed Description 141
10.57 rpki.exceptions.BSCNotReady Class Reference 141
10.57.1 Detailed Description 141
10.58 rpki.exceptions.ChildNotFound Class Reference 141
10.58.1 Detailed Description 142
10.59 rpki.exceptions.ClassNameMismatch Class Reference 142
10.59.1 Detailed Description 142
10.60 rpki.exceptions.ClassNameUnknown Class Reference 142
10.60.1 Detailed Description 142
10.61 rpki.exceptions.ClientNotFound Class Reference 142
10.61.1 Detailed Description 143
10.62 rpki.exceptions.CMSContentNotSet Class Reference 143
10.62.1 Detailed Description 143

10.63 rpki.exceptions.CMSCRLNotSet Class Reference 143
10.63.1 Detailed Description 143
10.64 rpki.exceptions.CMSVeri cationFailed Class Reference 143
10.64.1 Detailed Description 144
10.65 rpki.exceptions.DBConsistancyError Class Reference 144
10.65.1 Detailed Description 144
10.66 rpki.exceptions.DERObjectConversionError Class Reference . . 144
10.66.1 Detailed Description 144
10.67 rpki.exceptions.DuplicateObject Class Reference 144
10.67.1 Detailed Description 145
10.68 rpki.exceptions.EmptyPEM Class Reference 145
10.68.1 Detailed Description 145
10.69 rpki.exceptions.EmptyROAPre xList Class Reference 145
10.69.1 Detailed Description 145
10.70 rpki.exceptions.ForbiddenURI Class Reference 145
10.70.1 Detailed Description 146
10.71 rpki.exceptions.HandleTranslationError Class Reference 146
10.71.1 Detailed Description 146
10.72 rpki.exceptions.HTTPRequestFailed Class Reference 146
10.72.1 Detailed Description 146
10.73 rpki.exceptions.HTTPSBadVersion Class Reference 146
10.73.1 Detailed Description 147
10.74 rpki.exceptions.HTTPSClientAborted Class Reference 147
10.74.1 Detailed Description 147
10.75 rpki.exceptions.HTTPSUnexpectedState Class Reference 147
10.75.1 Detailed Description 147
10.76 rpki.exceptions.MissingCMSCRL Class Reference 147
10.76.1 Detailed Description 148
10.77 rpki.exceptions.MissingCMSEEcert Class Reference 148
10.77.1 Detailed Description 148
10.78 rpki.exceptions.MultipleTLSEECert Class Reference 148

10.78.1 Detailed Description 148
10.79 rpki.exceptions.MustBePre x Class Reference 148
10.79.1 Detailed Description 149
10.80 rpki.exceptions.NoActiveCA Class Reference 149
10.80.1 Detailed Description 149
10.81 rpki.exceptions.NoCoveringCertForROA Class Reference 149
10.81.1 Detailed Description 149
10.82 rpki.exceptions.NoObjectAtURI Class Reference 149
10.82.1 Detailed Description 150
10.83 rpki.exceptions.NotACerti cateChain Class Reference 150
10.83.1 Detailed Description 150
10.84 rpki.exceptions.NotFound Class Reference 150
10.84.1 Detailed Description 150
10.85 rpki.exceptions.NotImplementedYet Class Reference 150
10.85.1 Detailed Description 151
10.86 rpki.exceptions.NotInDatabase Class Reference 151
10.86.1 Detailed Description 151
10.87 rpki.exceptions.ReceivedTLSCACert Class Reference 151
10.87.1 Detailed Description 151
10.88 rpki.exceptions.RPKI_Exception Class Reference 151
10.88.1 Detailed Description 152
10.89 rpki.exceptions.ServerShuttingDown Class Reference 152
10.89.1 Detailed Description 152
10.90 rpki.exceptions.SKIMismatch Class Reference 153
10.90.1 Detailed Description 153
10.91 rpki.exceptions.SubprocessError Class Reference 153
10.91.1 Detailed Description 153
10.92 rpki.exceptions.TLSValidationError Class Reference 153
10.92.1 Detailed Description 153
10.93 rpki.exceptions.UnexpectedCMSCerts Class Reference 154
10.93.1 Detailed Description 154

10.94 rpki.exceptions.UnexpectedCMSCRLs Class Reference 154
10.94.1 Detailed Description 154
10.95 rpki.exceptions.UnparsableCMSDER Class Reference 154
10.95.1 Detailed Description 154
10.96 rpki.exceptions.UpstreamError Class Reference 155
10.96.1 Detailed Description 155
10.97 rpki.exceptions.WrongEContentType Class Reference 155
10.97.1 Detailed Description 155
10.98 rpki.https.http_client Class Reference 155
10.98.1 Detailed Description 156
10.98.2 Member Function Documentation 156
10.98.3 Member Data Documentation 158
10.99 rpki.https.http_listener Class Reference 160
10.99.1 Detailed Description 160
10.99.2 Member Function Documentation 160
10.99.3 Member Data Documentation 161
10.100 rpki.https.http_message Class Reference 162
10.100.1 Detailed Description 162
10.100.2 Member Function Documentation 163
10.100.3 Member Data Documentation 164
10.101 rpki.https.http_queue Class Reference 164
10.101.1 Detailed Description 165
10.101.2 Member Function Documentation 165
10.101.3 Member Data Documentation 166
10.102 rpki.https.http_request Class Reference 167
10.102.1 Detailed Description 167
10.102.2 Member Function Documentation 168
10.102.3 Member Data Documentation 168
10.103 rpki.https.http_response Class Reference 169
10.103.1 Detailed Description 169
10.103.2 Member Function Documentation 169

10.103.3 Member Data Documentation 170
10.104 rpki.https.http_server Class Reference 170
10.104.1 Detailed Description 171
10.104.2 Member Function Documentation 171
10.104.3 Member Data Documentation 172
10.105 rpki.https.http_stream Class Reference 173
10.105.1 Detailed Description 174
10.105.2 Member Function Documentation 175
10.105.3 Member Data Documentation 178
10.106 rpki.ipaddrs.v4addr Class Reference 179
10.106.1 Detailed Description 179
10.106.2 Member Function Documentation 180
10.106.3 Member Data Documentation 180
10.107 rpki.ipaddrs.v6addr Class Reference 181
10.107.1 Detailed Description 181
10.107.2 Member Function Documentation 181
10.107.3 Member Data Documentation 182
10.108 rpki.left_right.bsc_elt Class Reference 182
10.108.1 Detailed Description 183
10.108.2 Member Function Documentation 183
10.108.3 Member Data Documentation 184
10.109 rpki.left_right.child_elt Class Reference 186
10.109.1 Detailed Description 187
10.109.2 Member Function Documentation 187
10.109.3 Member Data Documentation 188
10.110 rpki.left_right.cms_msg Class Reference 190
10.110.1 Detailed Description 190
10.110.2 Member Data Documentation 191
10.111 rpki.left_right.data_elt Class Reference 191
10.111.1 Detailed Description 192
10.111.2 Member Function Documentation 192

10.111.3 Member Data Documentation 194
10.112 pki.left_right.left_right_namespace Class Reference 194
10.112.1 Detailed Description 194
10.112.2 Member Data Documentation 195
10.113 pki.left_right.list_published_objects_elt Class Reference 195
10.113.1 Detailed Description 196
10.113.2 Member Function Documentation 196
10.113.3 Member Data Documentation 196
10.114 pki.left_right.list_resources_elt Class Reference 197
10.114.1 Detailed Description 198
10.114.2 Member Function Documentation 198
10.114.3 Member Data Documentation 198
10.115 pki.left_right.list_roa_requests_elt Class Reference 199
10.115.1 Detailed Description 200
10.115.2 Member Function Documentation 200
10.115.3 Member Data Documentation 200
10.116 pki.left_right.msg Class Reference 201
10.116.1 Detailed Description 202
10.116.2 Member Function Documentation 202
10.116.3 Member Data Documentation 202
10.117 pki.left_right.parent_elt Class Reference 203
10.117.1 Detailed Description 203
10.117.2 Member Function Documentation 204
10.117.3 Member Data Documentation 205
10.118 pki.left_right.report_error_elt Class Reference 207
10.118.1 Detailed Description 208
10.118.2 Member Function Documentation 208
10.118.3 Member Data Documentation 208
10.119 pki.left_right.repository_elt Class Reference 209
10.119.1 Detailed Description 210
10.119.2 Member Function Documentation 210

10.119.3 Member Data Documentation 211
10.120 rpki.left_right.sax_handler Class Reference 212
10.120.1 Detailed Description 213
10.120.2 Member Data Documentation 213
10.121 rpki.left_right.self_elt Class Reference 213
10.121.1 Detailed Description 215
10.121.2 Member Function Documentation 215
10.121.3 Member Data Documentation 219
10.122 rpki.log.logger Class Reference 221
10.122.1 Detailed Description 221
10.122.2 Member Function Documentation 221
10.122.3 Member Data Documentation 222
10.123 rpki.manifest.FileAndHash Class Reference 222
10.123.1 Detailed Description 222
10.123.2 Member Function Documentation 222
10.123.3 Member Data Documentation 223
10.124 rpki.manifest.FilesAndHashes Class Reference 223
10.124.1 Detailed Description 223
10.124.2 Member Function Documentation 223
10.125 rpki.manifest.Manifest Class Reference 224
10.125.1 Detailed Description 224
10.125.2 Member Function Documentation 224
10.125.3 Member Data Documentation 224
10.126 rpki.publication.certi cate_elt Class Reference 225
10.126.1 Detailed Description 226
10.126.2 Member Data Documentation 226
10.127 rpki.publication.client_elt Class Reference 226
10.127.1 Detailed Description 227
10.127.2 Member Function Documentation 227
10.127.3 Member Data Documentation 228
10.128 rpki.publication.cms_msg Class Reference 230

10.128.1 Detailed Description . . . 230
10.128.2 Member Data Documentation . . . 230
10.129 rpki.publication.con g_elt Class Reference . . . 231
10.129.1 Detailed Description . . . 231
10.129.2 Member Function Documentation . . . 232
10.129.3 Member Data Documentation . . . 233
10.130 rpki.publication.control_elt Class Reference . . . 234
10.130.1 Detailed Description . . . 234
10.130.2 Member Function Documentation . . . 234
10.131 rpki.publication.crl_elt Class Reference . . . 235
10.131.1 Detailed Description . . . 235
10.131.2 Member Data Documentation . . . 235
10.132 rpki.publication.manifest_elt Class Reference . . . 235
10.132.1 Detailed Description . . . 236
10.132.2 Member Data Documentation . . . 236
10.133 rpki.publication.msg Class Reference . . . 236
10.133.1 Detailed Description . . . 237
10.133.2 Member Function Documentation . . . 237
10.133.3 Member Data Documentation . . . 237
10.134 rpki.publication.publication_namespace Class Reference . . . 238
10.134.1 Detailed Description . . . 238
10.134.2 Member Data Documentation . . . 238
10.135 rpki.publication.publication_object_elt Class Reference . . . 239
10.135.1 Detailed Description . . . 239
10.135.2 Member Function Documentation . . . 240
10.135.3 Member Data Documentation . . . 241
10.136 rpki.publication.report_error_elt Class Reference . . . 242
10.136.1 Detailed Description . . . 243
10.136.2 Member Function Documentation . . . 243
10.136.3 Member Data Documentation . . . 243
10.137 rpki.publication.roa_elt Class Reference . . . 245

10.137.1 Detailed Description . . . 245
10.137.2 Member Data Documentation . . . 245
10.138 rpki.publication.sax_handler Class Reference . . . 245
10.138.1 Detailed Description . . . 246
10.138.2 Member Data Documentation . . . 246
10.139 rpki.resource_set.resource_bag Class Reference . . . 246
10.139.1 Detailed Description . . . 247
10.139.2 Member Function Documentation . . . 247
10.139.3 Member Data Documentation . . . 249
10.140 rpki.resource_set.resource_range Class Reference . . . 250
10.140.1 Detailed Description . . . 250
10.140.2 Member Function Documentation . . . 251
10.140.3 Member Data Documentation . . . 251
10.141 rpki.resource_set.resource_range_as Class Reference . . . 251
10.141.1 Detailed Description . . . 252
10.141.2 Member Function Documentation . . . 252
10.141.3 Member Data Documentation . . . 252
10.142 rpki.resource_set.resource_range_ip Class Reference . . . 253
10.142.1 Detailed Description . . . 253
10.142.2 Member Function Documentation . . . 254
10.143 rpki.resource_set.resource_range_ipv4 Class Reference . . . 254
10.143.1 Detailed Description . . . 255
10.143.2 Member Data Documentation . . . 255
10.144 rpki.resource_set.resource_range_ipv6 Class Reference . . . 255
10.144.1 Detailed Description . . . 255
10.144.2 Member Data Documentation . . . 256
10.145 rpki.resource_set.resource_set Class Reference . . . 256
10.145.1 Detailed Description . . . 257
10.145.2 Member Function Documentation . . . 257
10.145.3 Member Data Documentation . . . 259
10.146 rpki.resource_set.resource_set_as Class Reference . . . 259

10.146.1 Detailed Description 260
10.146.2 Member Function Documentation 260
10.146.3 Member Data Documentation 261
10.147 rpki.resource_set.resource_set_ip Class Reference 261
10.147.1 Detailed Description 262
10.147.2 Member Function Documentation 262
10.147.3 Member Data Documentation 262
10.148 rpki.resource_set.resource_set_ipv4 Class Reference 263
10.148.1 Detailed Description 263
10.148.2 Member Data Documentation 263
10.149 rpki.resource_set.resource_set_ipv6 Class Reference 264
10.149.1 Detailed Description 264
10.149.2 Member Data Documentation 264
10.150 rpki.resource_set.roa_pre x Class Reference 265
10.150.1 Detailed Description 265
10.150.2 Member Function Documentation 265
10.150.3 Member Data Documentation 267
10.151 rpki.resource_set.roa_pre x_ipv4 Class Reference 267
10.151.1 Detailed Description 268
10.151.2 Member Data Documentation 268
10.152 rpki.resource_set.roa_pre x_ipv6 Class Reference 268
10.152.1 Detailed Description 268
10.152.2 Member Data Documentation 269
10.153 rpki.resource_set.roa_pre x_set Class Reference 269
10.153.1 Detailed Description 269
10.153.2 Member Function Documentation 269
10.154 rpki.resource_set.roa_pre x_set_ipv4 Class Reference 271
10.154.1 Detailed Description 271
10.154.2 Member Data Documentation 271
10.155 rpki.resource_set.roa_pre x_set_ipv6 Class Reference 272
10.155.1 Detailed Description 272

10.155.2 Member Data Documentation 272
10.156 rpki.roa.ROAIPAddress Class Reference 273
10.156.1 Detailed Description 273
10.156.2 Member Function Documentation 273
10.156.3 Member Data Documentation 273
10.157 rpki.roa.ROAIPAddresses Class Reference 274
10.157.1 Detailed Description 274
10.157.2 Member Function Documentation 274
10.158 rpki.roa.ROAIPAddressFamilies Class Reference 274
10.158.1 Detailed Description 275
10.158.2 Member Function Documentation 275
10.159 rpki.roa.ROAIPAddressFamily Class Reference 275
10.159.1 Detailed Description 275
10.159.2 Member Function Documentation 275
10.159.3 Member Data Documentation 276
10.160 rpki.roa.RouteOriginAttestation Class Reference 276
10.160.1 Detailed Description 276
10.160.2 Member Function Documentation 276
10.160.3 Member Data Documentation 277
10.161 rpki.rpki_engine.ca_detail_obj Class Reference 277
10.161.1 Detailed Description 278
10.161.2 Member Function Documentation 279
10.161.3 Member Data Documentation 283
10.162 rpki.rpki_engine.ca_obj Class Reference 285
10.162.1 Detailed Description 286
10.162.2 Member Function Documentation 287
10.162.3 Member Data Documentation 290
10.163 rpki.rpki_engine.child_cert_obj Class Reference 291
10.163.1 Detailed Description 292
10.163.2 Member Function Documentation 292
10.163.3 Member Data Documentation 294

10.164 rpki.rpki_engine.publication_queue Class Reference 295
10.164.1 Detailed Description 296
10.164.2 Member Function Documentation 296
10.164.3 Member Data Documentation 297
10.165 rpki.rpki_engine.revoked_cert_obj Class Reference 298
10.165.1 Detailed Description 298
10.165.2 Member Function Documentation 298
10.165.3 Member Data Documentation 299
10.166 rpki.rpki_engine.roa_obj Class Reference 300
10.166.1 Detailed Description 301
10.166.2 Member Function Documentation 301
10.166.3 Member Data Documentation 304
10.167 rpki.rpki_engine.rpkid_context Class Reference 306
10.167.1 Detailed Description 307
10.167.2 Member Function Documentation 307
10.167.3 Member Data Documentation 309
10.168 rpki.sql.session Class Reference 312
10.168.1 Detailed Description 313
10.168.2 Member Function Documentation 313
10.168.3 Member Data Documentation 315
10.169 rpki.sql.sql_persistent Class Reference 316
10.169.1 Detailed Description 317
10.169.2 Member Function Documentation 317
10.169.3 Member Data Documentation 321
10.170 rpki.sql.template Class Reference 322
10.170.1 Detailed Description 322
10.170.2 Member Function Documentation 323
10.170.3 Member Data Documentation 323
10.171 rpki.sundial.datetime Class Reference 324
10.171.1 Detailed Description 325
10.171.2 Member Function Documentation 325

10.171.3 Member Data Documentation 328
10.172 rpki.sundial.timedelta Class Reference 329
10.172.1 Detailed Description 329
10.172.2 Member Function Documentation 330
10.172.3 Member Data Documentation 332
10.173 rpki.up_down.base_elt Class Reference 332
10.173.1 Detailed Description 333
10.173.2 Member Function Documentation 333
10.174 rpki.up_down.certi cate_elt Class Reference 335
10.174.1 Detailed Description 335
10.174.2 Member Function Documentation 335
10.174.3 Member Data Documentation 336
10.175 rpki.up_down.class_elt Class Reference 337
10.175.1 Detailed Description 337
10.175.2 Member Function Documentation 338
10.175.3 Member Data Documentation 339
10.176 rpki.up_down.class_response_syntax Class Reference 340
10.176.1 Detailed Description 340
10.176.2 Member Function Documentation 341
10.176.3 Member Data Documentation 341
10.177 rpki.up_down.cms_msg Class Reference 341
10.177.1 Detailed Description 342
10.177.2 Member Data Documentation 342
10.178 rpki.up_down.error_response_pdu Class Reference 342
10.178.1 Detailed Description 343
10.178.2 Member Function Documentation 343
10.178.3 Member Data Documentation 344
10.179 rpki.up_down.issue_pdu Class Reference 345
10.179.1 Detailed Description 345
10.179.2 Member Function Documentation 346
10.179.3 Member Data Documentation 347

10.180 rpki.up_down.issue_response_pdu Class Reference 348
10.180.1 Detailed Description 348
10.180.2 Member Function Documentation 348
10.181 rpki.up_down.list_pdu Class Reference 348
10.181.1 Detailed Description 349
10.181.2 Member Function Documentation 349
10.182 rpki.up_down.list_response_pdu Class Reference 349
10.182.1 Detailed Description 350
10.183 rpki.up_down.message_pdu Class Reference 350
10.183.1 Detailed Description 351
10.183.2 Member Function Documentation 351
10.183.3 Member Data Documentation 352
10.184 rpki.up_down.multi_uri Class Reference 354
10.184.1 Detailed Description 354
10.184.2 Member Function Documentation 354
10.185 rpki.up_down.revoke_pdu Class Reference 355
10.185.1 Detailed Description 355
10.185.2 Member Function Documentation 355
10.185.3 Member Data Documentation 356
10.186 rpki.up_down.revoke_response_pdu Class Reference 356
10.186.1 Detailed Description 357
10.187 rpki.up_down.revoke_syntax Class Reference 357
10.187.1 Detailed Description 357
10.187.2 Member Function Documentation 357
10.187.3 Member Data Documentation 358
10.188 rpki.up_down.sax_handler Class Reference 358
10.188.1 Detailed Description 358
10.188.2 Member Data Documentation 359
10.189 rpki.x509.CMS_object Class Reference 359
10.189.1 Detailed Description 360
10.189.2 Member Function Documentation 361

10.189.3 Member Data Documentation 362
10.190 pki.x509.CRL Class Reference 364
10.190.1 Detailed Description 365
10.190.2 Member Function Documentation 365
10.190.3 Member Data Documentation 367
10.191 pki.x509.DeadDrop Class Reference 368
10.191.1 Detailed Description 368
10.191.2 Member Function Documentation 368
10.191.3 Member Data Documentation 369
10.192 pki.x509.DER_CMS_object Class Reference 369
10.192.1 Detailed Description 369
10.192.2 Member Function Documentation 370
10.192.3 Member Data Documentation 370
10.193 pki.x509.DER_object Class Reference 370
10.193.1 Detailed Description 371
10.193.2 Member Function Documentation 372
10.193.3 Member Data Documentation 376
10.194 pki.x509.PEM_converter Class Reference 377
10.194.1 Detailed Description 377
10.194.2 Member Function Documentation 378
10.194.3 Member Data Documentation 378
10.195 pki.x509.PKCS10 Class Reference 379
10.195.1 Detailed Description 379
10.195.2 Member Function Documentation 380
10.195.3 Member Data Documentation 381
10.196 pki.x509.ROA Class Reference 382
10.196.1 Detailed Description 382
10.196.2 Member Function Documentation 382
10.196.3 Member Data Documentation 382
10.197 pki.x509.RSA Class Reference 383
10.197.1 Detailed Description 384

10.197.2 Member Function Documentation 384
10.197.3 Member Data Documentation 385
10.198 pki.x509.RSApublic Class Reference 386
10.198.1 Detailed Description 387
10.198.2 Member Function Documentation 387
10.198.3 Member Data Documentation 387
10.199 pki.x509.SignedManifest Class Reference 388
10.199.1 Detailed Description 389
10.199.2 Member Function Documentation 389
10.199.3 Member Data Documentation 390
10.200 pki.x509.X509 Class Reference 390
10.200.1 Detailed Description 391
10.200.2 Member Function Documentation 391
10.200.3 Member Data Documentation 394
10.201 pki.x509.XML_CMS_object Class Reference 395
10.201.1 Detailed Description 396
10.201.2 Member Function Documentation 396
10.201.3 Member Data Documentation 397
10.202 pki.xml_utils.base_elt Class Reference 398
10.202.1 Detailed Description 399
10.202.2 Member Function Documentation 399
10.202.3 Member Data Documentation 401
10.203 pki.xml_utils.data_elt Class Reference 402
10.203.1 Detailed Description 402
10.203.2 Member Function Documentation 403
10.204 pki.xml_utils.msg Class Reference 406
10.204.1 Detailed Description 406
10.204.2 Member Function Documentation 407
10.204.3 Member Data Documentation 408
10.205 pki.xml_utils.sax_handler Class Reference 409
10.205.1 Detailed Description 409

10.205.2 Member Function Documentation . . . 409
10.205.3 Member Data Documentation . . . 411
10.206 rpki.xml_utils.text_elt Class Reference . . . 412
10.206.1 Detailed Description . . . 412
10.206.2 Member Function Documentation . . . 412
10.206.3 Member Data Documentation . . . 413
10.207 Sequence Class Reference . . . 413
10.208 SequenceOf Class Reference . . . 413
10.209 TextWrapper Class Reference . . . 413
10.210 ContentHandler Class Reference . . . 414

11 File Documentation 414
11.1 __init__.py File Reference . . . 414
11.2 async.py File Reference . . . 414
11.3 con g.py File Reference . . . 415
11.4 exceptions.py File Reference . . . 415
11.5 https.py File Reference . . . 416
11.6 ipaddrs.py File Reference . . . 417
11.7 irbe_cli.py File Reference . . . 418
11.8 irdbd.py File Reference . . . 419
11.9 left_right.py File Reference . . . 420
11.10 log.py File Reference . . . 420
11.11 manifest.py File Reference . . . 421
11.12 oids.py File Reference . . . 421
11.13 pubd.py File Reference . . . 422
11.14 publication.py File Reference . . . 422
11.15 relaxng.py File Reference . . . 423
11.16 resource_set.py File Reference . . . 423
11.17 roa.py File Reference . . . 424
11.18 rootd.py File Reference . . . 425
11.19 rpki_engine.py File Reference . . . 426

11.20 rpkid.py File Reference 427
11.21 sql.py File Reference 427
11.22 sundial.py File Reference 427
11.23 up_down.py File Reference 428
11.24 x509.py File Reference 428
11.25 xml_utils.py File Reference 429

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 certi cates. Most of the code is in the rpkid/rpki/ directory. rpkid itself is a relatively small program that calls the library modules. There are several other programs that make use of the same libraries, as well as a collection of test programs.

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

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

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

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

  - FreeBSD: /usr/ports/devel/py-lxml
  - Fedora: python-lxml.i386
  - Ubuntu: python-lxml

- http://sourceforge.net/projects/mysql-python/ . MySQLdb in turn requires MySQL client and server. rpkid et al have been tested with MySQL 5.0 and 5.1.
  - FreeBSD: /usr/ports/databases/py-MySQLdb
  - Fedora: MySQL-python.i386
  - Ubuntu: python-mysqldb

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

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

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

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

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

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

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

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

- http://pyyaml.org/ . testpoke.py (an up-down protocol command line test client) and testbed.py (a test harness) use PyYAML.
  - FreeBSD: /usr/ports/devel/py-yaml
  - Ubuntu: python-yaml

- http://xmlsoft.org/XSLT/ . Some of the test code uses xsltproc, from the Gnome LibXSLT package.
  - FreeBSD: /usr/ports/textproc/libxslt
  - Ubuntu: xsltproc
- http://w3m.sourceforge.net/ . testbed.py uses w3m to display the summary output from rcynic. Nothing terrible will happen if w3m isn't available, testbed.py will just complain about it being missing and won't display rcynic's output.
  - FreeBSD: /usr/ports/www/w3m
  - Ubuntu: w3m

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

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

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

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

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

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

- http://www.doxygen.org/ . Doxygen in turn pulls in several other tools, notably Graphviz, pdfLaTeX, and Ghostscript.
  - FreeBSD: /usr/ports/devel/doxygen
  - Ubuntu: doxygen
- http://lynx.isc.org/current/ . The documentation build process uses xsltproc and Lynx to dump at text versions of a few critical documentation pages.
  - FreeBSD: /usr/ports/www/lynx
  - Ubuntu: lynx

- http://www.thaiopensource.com/relaxng/trang.html . Trang is used to convert RelaxNG schemas from the human-readable "compact" form to the XML form that LibXML2 understands. Trang in turn requires Java.
  - FreeBSD: /usr/ports/textproc/trang
- http://search.cpan.org/dist/SQL-Translator/ . SQL-Translator, also known as "SQL Fairy", includes code to parse an SQL schema and dump a description of it as Graphviz input. SQL Fairy in turn requires Perl.
  - FreeBSD: /usr/ports/databases/p5-SQL-Translator

4 Operation Guide

Preliminary operation instructions for rpkid et al.

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

Warning:

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

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

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

- rpkid.py : The main RPKI engine daemon.
- pubd.py : The publication engine daemon.
- rootd.py : A separate daemon for handling the root of an RPKI certificate tree. This is essentially a stripped down version of rpkid with no SQL database, no left-right protocol implementation, and only the parent side of the up-down protocol. It's separate because the root is a special case in several ways and it was simpler to keep the special cases out of the main daemon.
- irdbd.py : A sample implementation of an IR database daemon. rpkid calls into this to perform lookups via the left-right protocol.
- irbe_cli.py : A command-line client for the left-right control protocol.

- cross_certify.py: A BPKI cross-certi cation tool.
- irbe-setup.py : An example of a script to set up the mappings between the IRDB and rpkid's own database, using the left-right control protocol.
- cronjob.py: A trivial HTTP client used to drive rpkid cron events.
- testbed.py: A test tool for running a collection of rpkid and irdb instances under common control, driven by a uni ed test script.
- testpoke.py: A simple client for the up-down protocol, mostly compatable with APNIC's rpki_poke.pl tool.

Most of these programs take con guration les 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 con guration les which may be useful as examples.

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

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

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

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

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

4.1 rpkid.py

rpkid is the main RPKI engine daemon. Con guration of rpkid is a two step process: a con g le to bootstrap rpkid to the point where it can speak using the left-right protocol, followed by dynamic con guration via the left-right protocol. In production use the latter stage would be handled by the IRBE stub; for test and develoment purposes it's handled by the irbe_cli.py command line interface or by the testbed.py test framework.

rpkid stores dynamic data in an SQL database, which must have been created for it, as explained in the installation guide.

The default con g le is rpkid.conf, start rpkid with "-c lename" to choose a different con g le. All options are in the section "[rpkid]". Certi cates, keys, and trust anchors may be in either DER or PEM format.

Con g le options:

- startup-message : String to log on startup, useful when debugging a collection of rpkid instances at once.
- sql-username : Username to hand to MySQL when connecting to rpkid's database.
- sql-database : MySQL's database name for rpkid's database.
- sql-password : Password to hand to MySQL when connecting to rpkid's database.
- bpki-ta : Name of le containing BPKI trust anchor. All BPKI certi cate veri cation within rpkid traces back to this trust anchor.
- rpkid-cert : Name of le containing rpkid's own BPKI EE certi cate.
- rpkid-key : Name of le containing RSA key corresponding to rpkid-cert.
- irbe-cert : Name of le containing BPKI certi cate used by IRBE when talking to rpkid.
- irdb-cert : Name of le containing BPKI certi cate 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 implmenetation 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 implemntation 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, basicly) 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 le containing BPKI trust anchor. All BPKI certi cate validation in irdbd traces back to this trust anchor.
- irdbd-cert : Name of le containing irdbd's own BPKI certi cate.
- irdbd-key : Name of le containing RSA key corresponding to irdbd-cert.
- rpkid-cert : Name of le containing certi cate used the one and only by rpkid instance authorized to contact this irdbd instance.
- https-url : Service URL for irdbd. Must be a https:// URL.

4.5 irbe_cli.py

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

Basic con guration of irbe_cli is handled via a con g le. The speci c action or actions to be performed are speci ed 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 speci ed on the command line, any PKCS #10 requests received from rpkid will be written in PEM format to that le; this makes it easier to hand these requests off to the business PKI (BPKI in order to issue signing certs corresponding to newly generated business keys.

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

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

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

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

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

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

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

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

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

Usage:

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

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

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

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

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

-- *_handle options refer to object primary keys.

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

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

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

Configuration 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 "[irdbd]". Certificates, keys, and trust anchors may be in either DER or PEM format.

Options in the "[irbe_cli]" section:

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

Options in the "[irdbd]" section:

- 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.

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 con g le is cronjob.conf, start cronjob with "-c lename" to choose a different con g le. All options are in the section "[cronjob]". Certi cates, keys, and trust anchors may be in either DER or PEM format.

Con g le options:

- bpki-ta : Name of le containing BPKI trust anchor.
- irbe-cert : Name of le containing cronjob.py's BPKI certi cate.
- https-key : Name of le containing RSA key corresponding to irbe-cert.
- rpkid-cert : Name of le containing rpkid's BPKI certi cate.
- 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 con guration les in different languages. The rst con guration le uses the same syntax as the above con guration les but is completely optional. The second con guration le 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 con gurations 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 in the rst (optional) con guration le are just overrides for wired-in default values. In most cases the defaults will suf ce, and the set of options is still

in ux, so only a few of the options are described here. The default name for this con guration le is testbed.conf, run testbed with "-c lename" to change it.

testbed.conf options:

- testbed_dir: Working directory into which testbed should write the (many) les 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 ctious) directory to use as the id-ad-caRepository SIA value in the generated root resource certi cate. 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 con guration le is named testbed.yaml by default, run testbed with "-y lename" to change it. The YAML le contains multiple YAML "documents". The rst document describes the initial test layout and resource allocations, subsequent documents describe modi cations 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 modi cations to the current resource set, modi cations 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 speci es 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 rst subsequent document adds ten seconds to the validity interval for Alice's resources and makes no other modi cations. 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 nal 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 speci ed 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 elds are optional, but at least one must be speci ed. 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 con g le in OpenSSL-compatable format at all. Instead, it is con gured exclusively by a YAML script. testpoke's design was constrained

by a desire to have it be compatable with APNIC's rpki_poke.pl tool, so that the two tools could use a common con guration language to simplify scripted testing. There are minor variations due to slightly different feature sets, but YAML les intended for one program will usually work with the other.

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

testpoke.py takes a simpli ed command line and uses only one YAML input le.

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

Default con guration le is testpoke.yaml, override with --yaml option.

The --request option speci es the speci c command within the YAML le to execute.

Sample con guration le:

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

version: 1
posturl: https://localhost:4433/up-down/1
recipient-id: wombat
sender-id: "1"

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

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

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

testpoke adds one extension to the language described in APNIC's README: the cms-cert-chain- and ssl-cert-chain-options, which allow one to specify a chain of

intermediate certi cates to be presented in the CMS or TLS protocol. APNIC's initial implementation required direct knowledge of the issuing certi cate (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 certi cates.

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 protcol uses a kind of message-passing. Each object that the RPKI engine knows about takes ve 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 elds to be set. For example, to generate a keypair one "sets" the "generate-keypair" eld of a BSC object, even though there is no such eld 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 elds, 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 elds 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 id-ct-xml

(1.2.840.113549.1.9.16.1.28). These CMS messages are in turn passed as the data for HTTPS POST operations, with an HTTP content type of "application/x-rpki" for both the POST data and the response data.

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

5.2.1 <self/> object

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

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

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

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

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

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

bpki_glue certi cate; otherwise, the bpki_cert certi cate should be issued by the per-engine bpki_ta certi cate.

- bpki_glue (element): Another BPKI CA certi cate for this <self/>, usually not needed. Certain pathological cross-certi cation cases require a two-certi cate chain due to issuer name con icts. If used, the bpki_glue certi cate should be the issuer of the bpki_cert certi cate and should be issued by the per-engine bpki_ta certi cate; if not needed, the bpki_glue certi cate 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 rst phase of a key rollover operation.

- revoke: Revoke any remaining certi cates 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 rst phase to leave time for new RPKI certi cates to propegate 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 con guration decision based on external requirements: the RPKI engine code doesn't care, it just cares that, for any object representing a relationship for which it must sign messages, there be a <bsc/> object that it can use to produce that signature.

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

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

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

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

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

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

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

Replies to "create" and "set" actions that specify "generate-keypair" include a <bsc_pkcs10/> element, as do replies to "get" and "list" actions for a <bsc/> object for which a "generate-keypair" command has been issued. The RPKI engine stores the PKCS #10 request, which allows the IRBE to reuse the request if and when it needs to reissue the corresponding BPKI signing certificate.

5.2.3 <parent/> object

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

Every <parent/> object has a parent_handle, which must be specified for the "create", "get", "set", and "destroy" actions. Every <parent/> also has a self_handle

attribute which indicates the <self/> object with which this <parent/> object is associated, a bsc_handle attribute indicating the <bsc/> object to be used when signing messages sent to this parent, and a repository_handle indicating the <repository/> object to be used when publishing issued by the certificate issued by this parent.

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

- peer_contact_uri (attribute): HTTPS URI used to contact this parent.
- sia_base (attribute): The leading portion of an rsync URI that the RPKI engine should use when composing the publication URI for objects issued by the RPKI certificate issued by this parent.
- sender_name (attribute): Sender name to use in the up-down protocol when talking to this parent. The RPKI engine doesn't really care what this value is, but other implementations of the up-down protocol do care.
- recipient_name (attribute): Recipient name to use in the up-down protocol when talking to this parent. The RPKI engine doesn't really care what this value is, but other implementations of the up-down protocol do care.
- bpki_cms_cert (element): BPKI CMS CA certificate for this <parent/>. This is used as part of the certificate chain when validating incoming CMS messages If the bpki_cms_glue certificate is in use (below), the bpki_cms_cert certificate should be issued by the bpki_cms_glue certificate; otherwise, the bpki_cms_cert certificate should be issued by the bpki_cert certificate in the <self/> object.
- bpki_cms_glue (element): Another BPKI CMS CA certificate for this <parent/>, usually not needed. Certain pathological cross-certification cases require a two-certificate chain due to issuer name conflicts. If used, the bpki_cms_glue certificate should be the issuer of the bpki_cms_cert certificate and should be issued by the bpki_cert certificate in the <self/> object; if not needed, the bpki_cms_glue certificate should be left unset.
- bpki_https_cert (element): BPKI HTTPS CA certificate for this <parent/>. This is like the bpki_cms_cert object, only used for validating incoming TLS messages rather than CMS.
- bpki_cms_glue (element): Another BPKI HTTPS CA certificate for this <parent/>, usually not needed. This is like the bpki_cms_glue certificate, only used for validating incoming TLS messages rather than CMS.

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

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

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

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

5.2.4 <child/> object

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

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

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

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

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

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

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

5.2.5 <repository/> object

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

Every <repository/> object has a repository_handle, which must be specified for the "create", "get", "set", and "destroy" actions. Every <repository/> also

has a self_handle attribute which indicates the <self/> object with which this <repository/> object is associated.

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

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

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

5.2.6 <route_origin/> object

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

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

Note that a <route_origin/> object represents a ROA to be generated on behalf of <self/>, not on behalf of a <child/>. Thus, a hosted entity that has no children but which does need to generate ROAs would be represented by a hosted <self/> with no <child/> objects but one or more <route_origin/> objects. While lumping ROA generation in with the other RPKI engine activities may

seem a little odd at rst, 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 certi cate must also be the engine which generates any ROAs that derive from that RPKI certi cate.

The precise content of the <route_origin/> has changed over time as the underlying ROA speci cation 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 pre x and maxLength encoding used in the -03 draft.

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

- asn (attribute): Autonomous System Number (ASN) to place in the generated ROA. A single ROA can only grant authorization to a single ASN; multiple ASNs require multiple ROAs, thus multiple <route_origin/> objects.
- ipv4 (attribute): List of IPv4 pre x and maxLength values, see below for format.
- ipv6 (attribute): List of IPv6 pre x 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 pre x and maxLength values are represented as comma-separated text strings, with no whitespace permitted. Each entry in such a string represents a single pre x/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 certi cates will be different as the back-queries and responses form a separate communication channel.

5.3.1 <list_resources/> messages

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

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

- valid_until: A timestamp indicating the date and time at which certi cates 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" suf x 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 pre xes and ranges, expressed as a comma-separated list of pre xes and ranges with no whitespace. See below for format details.

- ipv6: A list of IPv6 address pre xes and ranges, expressed as a comma-separated list of pre xes and ranges with no whitespace. See below for format details.

Entries in a list of address pre xes and ranges can be either pre xes, which are written in the usual address/pre xlen 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 super cially similar to the format used for pre x 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 speci cation.

5.4 Error handling

Error in this protocol are handled at two levels.

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

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

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

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

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

The body of the <report_error/> element itself is an optional text string; if present, this is debugging information. At present this capabilty 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. Con gured 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 <con g/> object

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

There is exactly one <con g/> 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 con gured in a <con g/> object:

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

6.2.2 <client/> object

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

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

Payload data which can be con gured 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 certi cate for this <client/>. This is used as part of the certi cate chain when validating incoming TLS and CMS messages. If the bpki_glue certi cate is in use (below), the bpki_cert certi cate should be issued by the bpki_glue certi cate; otherwise, the bpki_cert certi cate should be issued by the publication engine's bpki_ta certi cate.

- bpki_glue (element): Another BPKI CA certi cate for this <client/>, usually not needed. Certain pathological cross-certi cation cases require a two-certi cate chain due to issuer name con icts. If used, the bpki_glue certi cate should be the issuer of the bpki_cert certi cate and should be issued by the publication engine's bpki_ta certi cate; if not needed, the bpki_glue certi cate 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 hte 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 <certi cate/> object

The <certi cate/> object represents an RPKI certi cate 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 capabilty 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 certi cate pro le requires the child's publication point to be indicated in an SIA extension in a certi cate issued by the parent to the child, the publication engine can infer this permission from the parent's issuance of a certi cate to the child. Since, by de nition, the parent also uses this publication server, this is an easy check, as the publication server should already have the parent's certi cate available by the time it needs to check the child's certi cate.

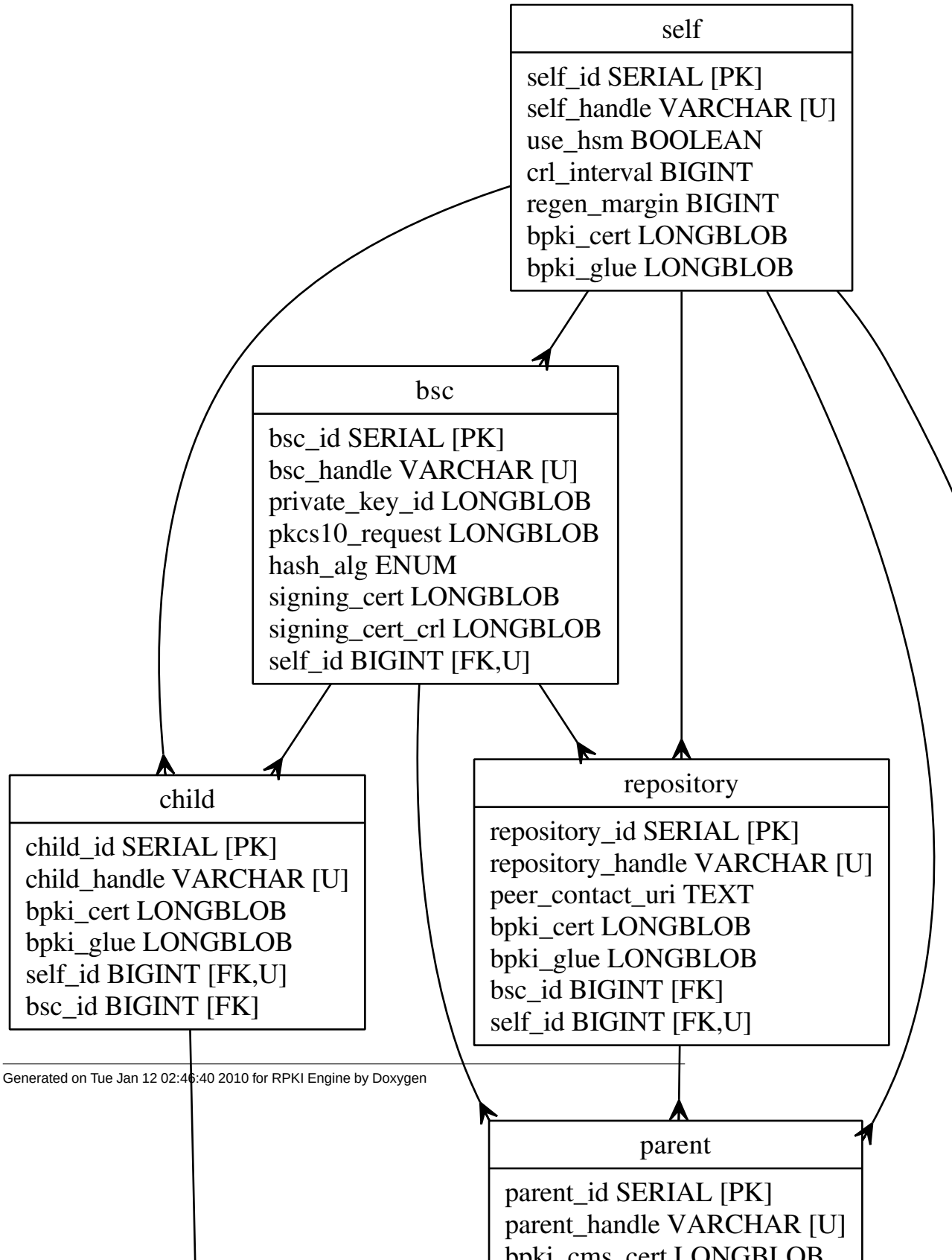
The previous paragraph only covers a "publish" action for a <certificate/> object. For "publish" actions on other objects, the publication server would need to trace permission back to the certi cate issued by the parent; for "withdraw" actions, the publication server would have to perform the same checks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

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

7 SQL database schemas

- rpkid database schema
- pubd database schema
- irdbd database schema

7.1 rpkid SQL schema



```
-- $Id: rpkid.sql 2906 2009-12-23 06:31:32Z 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.

-- SQL objects needed by the RPKI engine (rpkid.py).

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

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

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

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

```
        UNIQUE                  (self_id, bsc_handle)
) ENGINE=InnoDB;

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

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

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

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

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

CREATE TABLE child_cert (
        child_cert_id           SERIAL NOT NULL,
        cert                       LONGBLOB NOT NULL,
        published                 DATETIME,
        ski                        TINYBLOB NOT NULL,
        child_id                BIGINT UNSIGNED NOT NULL,
        ca_detail_id            BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY                (child_cert_id),
        CONSTRAINT                 child_cert_ca_detail_id
        FOREIGN KEY                (ca_detail_id) REFERENCES ca_detail (ca_detail_id) ON DELETE CASCADE,
        CONSTRAINT                 child_cert_child_id
        FOREIGN KEY                (child_id) REFERENCES child (child_id) ON DELETE CASCADE
) ENGINE=InnoDB;

CREATE TABLE revoked_cert (
        revoked_cert_id         SERIAL NOT NULL,
        serial                   BIGINT UNSIGNED NOT NULL,
        revoked                    DATETIME NOT NULL,
        expires                   DATETIME NOT NULL,
        ca_detail_id            BIGINT UNSIGNED NOT NULL,
        PRIMARY KEY                (revoked_cert_id),
```

```
        CONSTRAINT              revoked_cert_ca_detail_id
        FOREIGN KEY             (ca_detail_id) REFERENCES ca_detail (ca_detail_id) ON DELETE CASCADE
) ENGINE=InnoDB;

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

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

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

7.2 pubd SQL Schema

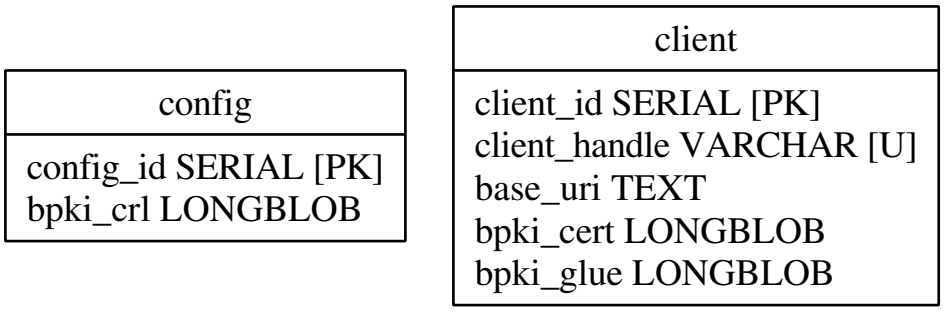


Figure 2: Diagram of pubd.sql

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

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

-- SQL objects needed by pubd.py.

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

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

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

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

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

7.3 irdbd SQL Schema

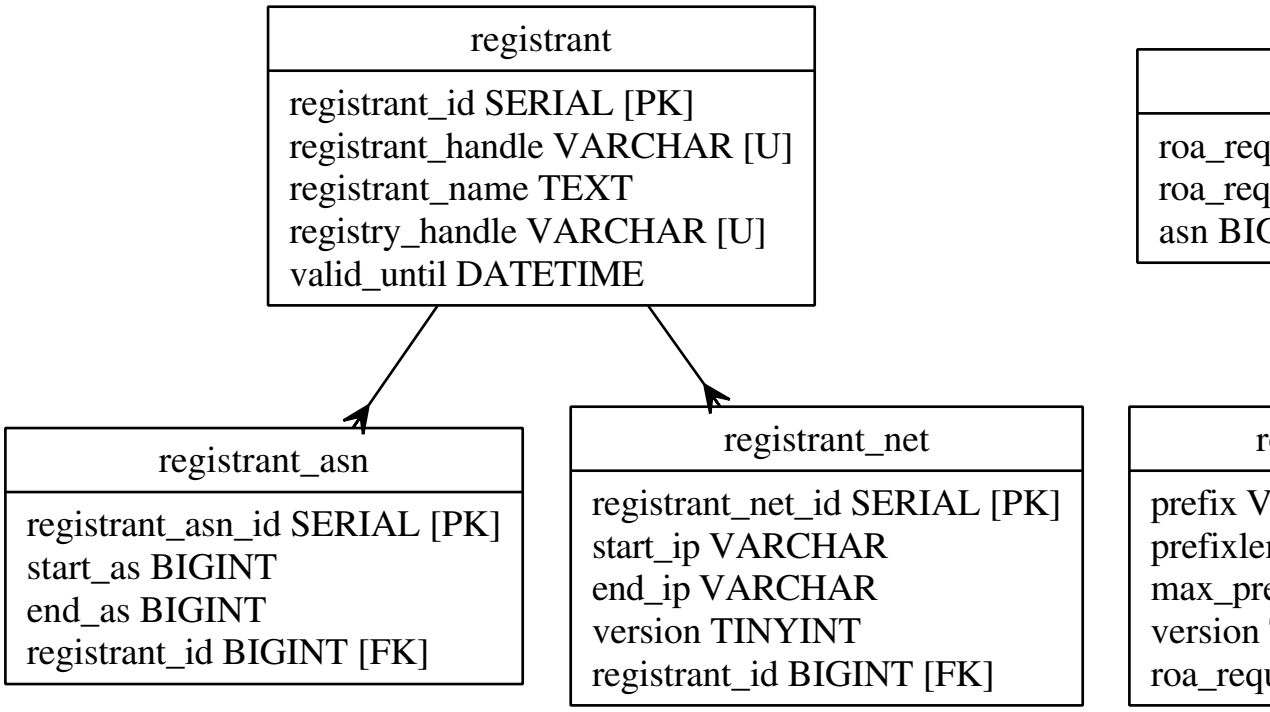


Figure 3: Diagram of irdbd.sql

```
-- $Id: irdbd.sql 2906 2009-12-23 06:31:32Z 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.

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

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

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

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

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

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

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

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

```
) ENGINE=InnoDB;

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

8 BPKI model

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

BPKI certi cates are not resource PKI (RPKI) certi cates. 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".

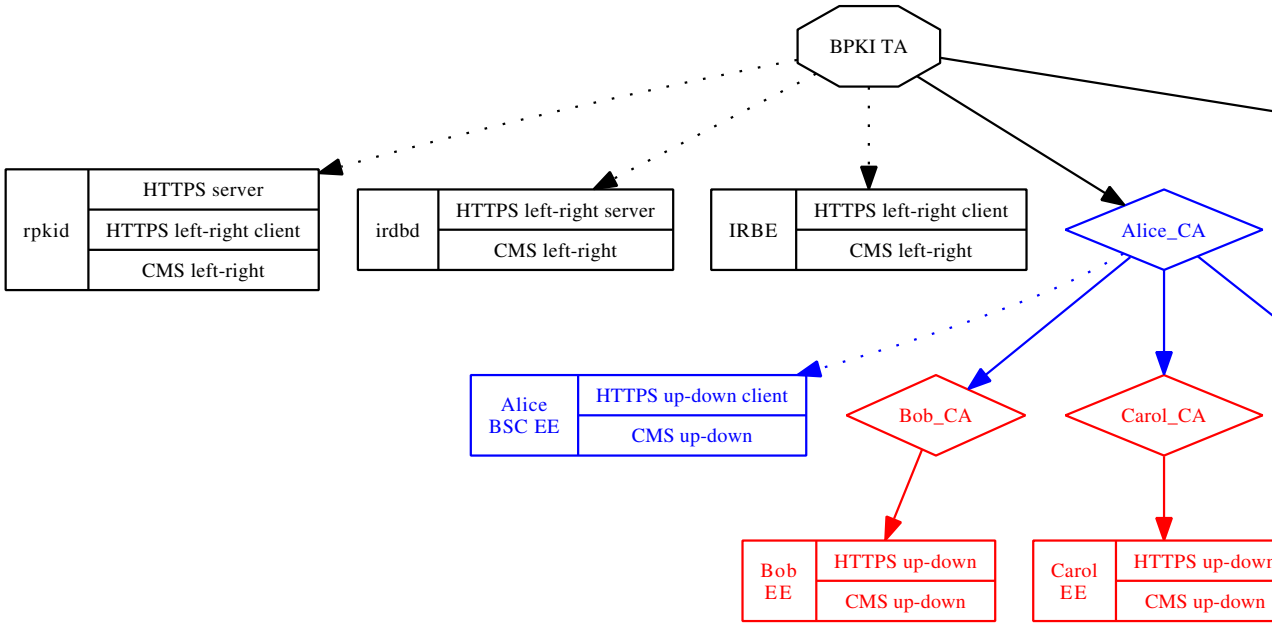
Setup of the BPKI is handled by the back end; for the most part, rpkid and pubd just use the result. The one place where the engines are directly involved in creation of new BPKI certi cates is in the production of end-entity certi cates for use by the engines.

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-certi ed into the engine's BPKI tree.
- Private keys must never transit the network.
- Except for end entity certi cates, the engine should only have access to the BPKI certi cates; in particular, the private key for the BPKI trust anchor should not be accessible to the engine.
- The number of BPKI keys and certi cates 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 certi cate hierarchy within rpkid.

Here is a simpli ed 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-certi ed objects from the hosted entities' peers. The arrows indicate certi cate issuance: solid arrows are the ones rpkid will care about during certi cate validation, dotted arrows show the origin of the EE certi cates that rpkid uses to sign CMS and TLS messages.

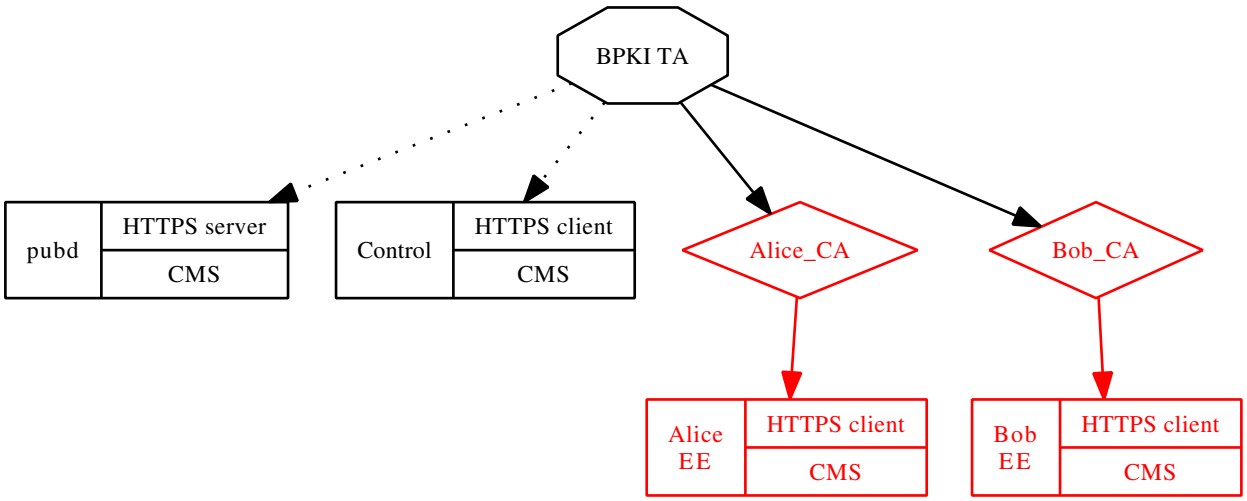
There's one nasty bit where the model had to bend to t the current state of the underlying protocols: it's not possible to use exactly the same BPKI keys and certi cates for HTTPS and CMS. The reason for this is simple: each hosted entity has its own BPKI, as does the hosting entity, but the HTTPS listener is shared. The only ways to avoid sharing the HTTPS server certi cate 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 certi cate tree looks complicated, but the set of certi cates needed to build any particular validation chain is obvious, again excepting the HTTPS server case, where the client certi cate is the rst hint that the engine has of the client's identity, so the server must be prepared to accept any current client certi cate.

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 speci cally for the purpose of generating the cross-certi cation certi cates 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 a 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 simpli ed picture of what the BPKI might look like for a pubd operator that serves two clients, "Alice" and "Bob":



While it is likely that RIRs (at least) will operate both rpkid and pubd instances, the two functions are conceptually separate. As far as pubd is concerned, it doesn't matter who operates the rpkid instance; pubd just has clients, each of which has trust material that has been cross-certi ed into pubd's BPKI. Similarly, rpkid doesn't really care who operates a pubd instance that it's been con gured to use, it just treats that pubd as a foreign BPKI whose trust material has to be cross-certi ed into its own BPKI. Cross certi cation itself is done by the back end operator, using cross_certify or some equivalent tool; the resulting BPKI certi cates are con gured into rpkid and pubd via the left-right protocol and the control subprotocol of the publication protocol, respectively.

Because the BPKI tree is almost entirely controlled by the operating entity, CRLs are not necessary for most of the BPKI. The one exception to this is the EE certi cates issued under the cross-certi cation points. These EE certi cates are generated by the peer, not the local operator, and thus require CRLs. Because of this, both rpkid and pubd require regular updates of certain BPKI CRLs, again via the left-right and publication control protocols.

Because the left-right protocol and the publication control subprotocol are used to con gure BPKI certi cates and CRLs, they cannot themselves use certi cates and CRLs con gured in this way. This is why the con guration les for rpkid and pubd require static con guration of the left-right and publication control certi cates.

9 Namespace Documentation

9.1 Package irbe_cli

Classes

- class bsc_elt
- class caller
- class certi cate_elt
- class child_elt
- class client_elt
- class cmd_elt_mixin
- class cmd_msg_mixin
- class con g_elt
- class crl_elt
- class left_right_cms_msg
- class left_right_msg
- class left_right_sax_handler
- class list_published_objects_elt
- class manifest_elt
- class parent_elt
- class publication_cms_msg
- class publication_msg
- class publication_sax_handler
- class reply_elt_mixin
- class report_error_elt
- class repository_elt
- class roa_elt
- class self_elt
- class UsageWrapper

Functions

- def usage

Variables

- list argv = sys.argv[1:]
- tuple call_pubd
- tuple call_rpkid
- tuple cfg = rpki.con g.parse(cfg_ le, "irbe_cli")
- string cfg_ le = "irbe.conf"

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

9.1.1 Detailed Description

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

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

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

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

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

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

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

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

9.1.2 Function Documentation

9.1.2.1 def irbe_cli.usage(code = 1)

De nition at line 275 of le irbe_cli.py.

9.1.3 Variable Documentation

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

De nition at line 294 of le irbe_cli.py.

9.1.3.2 tuple irbe_cli.call_pubd

Initial value:

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

De nition at line 349 of le irbe_cli.py.

9.1.3.3 tuple irbe_cli.call_rpkid

Initial value:

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

De nition at line 337 of le irbe_cli.py.

9.1.3.4 tuple irbe_cli.cfg = rpki.con g.parser(cfg_ le, "irbe_cli")

De nition at line 318 of le irbe_cli.py.

9.1.3.5 irbe_cli.cfg_ le = "irbe.conf"

De nition at line 299 of le irbe_cli.py.

9.1.3.6 irbe_cli.pem_out = None

De nition at line 39 of le irbe_cli.py.

9.1.3.7 irbe_cli.q_msg = q_msg_left_right

De nition at line 326 of le irbe_cli.py.

9.1.3.8 tuple irbe_cli.q_msg_left_right = left_right_msg.query()

De nition at line 320 of le irbe_cli.py.

9.1.3.9 tuple irbe_cli.q_msg_publication = publication_msg.query()

De nition at line 321 of le irbe_cli.py.

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

De nition at line 325 of le irbe_cli.py.

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

De nition at line 273 of le irbe_cli.py.

9.1.3.12 tuple irbe_cli.usage_ ll = UsageWrapper(subsequent_indent = " ⁎ 4)

De nition at line 87 of le irbe_cli.py.

9.1.3.13 irbe_cli.verbose = True

De nition at line 300 of le irbe_cli.py.

9.2 Package irdbd

Functions

- def handle_list_resources
- def handle_list_roa_requests
- def handler

Variables

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

9.2.1 Detailed Description

IR database daemon.

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

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

$Id: irdbd.py 2913 2009-12-28 20:55:38Z sra $

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

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

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

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

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

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

9.2.2 Function Documentation

9.2.2.1 def irdbd.handle_list_resources(q_pdu, r_msg)

De nition at line 53 of le irdbd.py.

9.2.2.2 def irdbd.handle_list_roa_requests(q_pdu, r_msg)

De nition at line 90 of le irdbd.py.

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

De nition at line 119 of le irdbd.py.

9.2.3 Variable Documentation

9.2.3.1 tuple irdbd.bpki_ta = rpki.x509.X509(Auto_ le = cfg.get("bpki-ta"))

De nition at line 201 of le irdbd.py.

9.2.3.2 tuple irdbd.cfg = rpki.con g.parser(cfg_ le, "irdbd")

De nition at line 186 of le irdbd.py.

9.2.3.3 irdbd.cfg_ le = "irdbd.conf"

De nition at line 170 of le irdbd.py.

9.2.3.4 tuple irdbd.client_ta = (bpki_ta, rpkid_cert)

De nition at line 217 of le irdbd.py.

9.2.3.5 tuple irdbd.cur = db.cursor()

De nition at line 198 of le irdbd.py.

9.2.3.6 tuple irdbd.db

Initial value:

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

De nition at line 194 of le irdbd.py.

9.2.3.7 dictionary irdbd.handle_dispatch

Initial value:

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

De nition at line 115 of le irdbd.py.

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

De nition at line 220 of le irdbd.py.

9.2.3.9 string irdbd.host = "localhost"

De nition at line 218 of le irdbd.py.

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

De nition at line 203 of le irdbd.py.

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

De nition at line 204 of le irdbd.py.

9.2.3.12 int irdbd.port = 443

De nition at line 219 of le irdbd.py.

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

De nition at line 202 of le irdbd.py.

9.2.3.14 irdbd.server_cert = irdbd_cert,

De nition at line 216 of le irdbd.py.

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

De nition at line 188 of le irdbd.py.

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

De nition at line 206 of le irdbd.py.

9.3 Package pubd

Classes

- class pubd_context

Functions

- def main

Variables

- string cfg_ le = "pubd.conf"
- pro le = False

9.3.1 Detailed Description

RPKI publication engine.

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

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

$Id: pubd.py 2913 2009-12-28 20:55:38Z sra $

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

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

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

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

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

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

9.3.2 Function Documentation

9.3.2.1 def pubd.main ()

De nition at line 172 of le pubd.py.

9.3.3 Variable Documentation

9.3.3.1 pubd.cfg_ le = "pubd.conf"

De nition at line 153 of le pubd.py.

9.3.3.2 pubd.pro le = False

De nition at line 154 of le pubd.py.

9.4 Package rootd

Classes

- class cms_msg
- class issue_pdu
- class list_pdu
- class message_pdu
- class revoke_pdu
- class sax_handler

Functions

- def compose_response
- def del_subject_cert
- def del_subject_pkcs10
- def get_root_cert
- def get_subject_cert
- def get_subject_pkcs10
- def issue_subject_cert_maybe
- def root_newer_than_subject
- def set_subject_cert
- def set_subject_pkcs10
- def up_down_handler

Variables

- tuple bpki_ta = rpki.x509.X509(Auto_ le = cfg.get("bpki-ta"))
- tuple cfg = rpki.con g.parser(cfg_ le , "rootd")
- string cfg_ le = "rootd.conf"
- tuple child_bpki_cert = rpki.x509.X509(Auto_ le = 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_ le = cfg.get("rootd-bpki-cert"))
- tuple rootd_bpki_crl = rpki.x509.CRL(Auto_ le = cfg.get("rootd-bpki-crl"))
- tuple rootd_bpki_key = rpki.x509.RSA(Auto_ le = cfg.get("rootd-bpki-key"))
- tuple rpki_base_uri = cfg.get("rpki-base-uri", "rsync://" + rpki_class_name + ".invalid/")

- tuple rpki_class_name = cfg.get("rpki-class-name", "wombat")
- rpki_root_cert = None
- tuple rpki_root_cert_ le = 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_ le = cfg.get("rpki-root-key"))
- tuple rpki_root_manifest = cfg.get("rpki-root-manifest", "Root.mnf")
- tuple rpki_subject_cert = cfg.get("rpki-subject-cert", "Child.cer")
- tuple rpki_subject_lifetime = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-lifetime", "30d"))
- tuple rpki_subject_pkcs10 = cfg.get("rpki-subject-pkcs10", "Child.pkcs10")
- tuple rpki_subject_regen = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-regen", rpki_subject_lifetime.convert_to_seconds() / 2))
- server_cert = rootd_bpki_cert

9.4.1 Detailed Description

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

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

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

$Id: rootd.py 2913 2009-12-28 20:55:38Z sra $

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

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

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

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

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

THE SOFTWARE IS PROVIDED "AS IS" AND ARIN DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY

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

9.4.2 Function Documentation

9.4.2.1 def rootd.compose_response (msg, pkcs10 = None)

De nition at line 175 of le rootd.py.

9.4.2.2 def rootd.del_subject_cert ()

De nition at line 72 of le rootd.py.

9.4.2.3 def rootd.del_subject_pkcs10 ()

De nition at line 91 of le rootd.py.

9.4.2.4 def rootd.get_root_cert ()

De nition at line 48 of le rootd.py.

9.4.2.5 def rootd.get_subject_cert ()

De nition at line 56 of le rootd.py.

9.4.2.6 def rootd.get_subject_pkcs10 ()

De nition at line 77 of le rootd.py.

9.4.2.7 def rootd.issue_subject_cert_maybe_new(new_pkcs10)

De nition at line 98 of le rootd.py.

9.4.2.8 def rootd.root_newer_than_subject ()

De nition at line 53 of le rootd.py.

9.4.2.9 def rootd.set_subject_cert(cert)

De nition at line 65 of le rootd.py.

9.4.2.10 def rootd.set_subject_pkcs10(pkcs10)

De nition at line 85 of le rootd.py.

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

De nition at line 238 of le rootd.py.

9.4.3 Variable Documentation

9.4.3.1 tuple rootd.bpki_ta = rpki.x509.X509(Auto_ le = cfg.get("bpki-ta"))

De nition at line 288 of le rootd.py.

9.4.3.2 tuple rootd.cfg = rpki.con g.parser(cfg_ le, "rootd")

De nition at line 284 of le rootd.py.

9.4.3.3 rootd.cfg_ le = "rootd.conf"

De nition at line 268 of le rootd.py.

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

De nition at line 292 of le rootd.py.

9.4.3.5 tuple rootd.client_ta = (bpki_ta, child_bpki_cert)

De nition at line 316 of le rootd.py.

9.4.3.6 rootd.handlers = up_down_handler)

De nition at line 319 of le rootd.py.

9.4.3.7 rootd.host = https_server_host,

De nition at line 317 of le rootd.py.

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

De nition at line 294 of le rootd.py.

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

De nition at line 295 of le rootd.py.

9.4.3.10 rootd.port = https_server_port,

De nition at line 318 of le rootd.py.

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

De nition at line 290 of le rootd.py.

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

De nition at line 291 of le rootd.py.

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

De nition at line 289 of le rootd.py.

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

De nition at line 300 of le rootd.py.

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

De nition at line 297 of le rootd.py.

9.4.3.16 rootd.rpki_root_cert = None

De nition at line 46 of le rootd.py.

9.4.3.17 tuple rootd.rpki_root_cert_ le = cfg.get("rpki-root-cert")

De nition at line 303 of le rootd.py.

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

De nition at line 304 of le rootd.py.

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

De nition at line 307 of le rootd.py.

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

De nition at line 299 of le rootd.py.

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

De nition at line 302 of le rootd.py.

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

De nition at line 306 of le rootd.py.

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

De nition at line 308 of le rootd.py.

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

De nition at line 311 of le rootd.py.

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

De nition at line 309 of le rootd.py.

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

De nition at line 312 of le rootd.py.

9.4.3.27 rootd.server_cert = rootd_bpki_cert,

De nition at line 315 of le rootd.py.

9.5 Package rpki

Packages

- package async
- package con g
- package exceptions
- package https
- package ipaddrs
- package left_right
- package log
- package manifest
- package oids
- package publication

- package relaxng
- package resource_set
- package roa
- package rpki_engine
- package sql
- package sundial
- package up_down
- package x509
- package xml_utils

9.6 Package rpki.async

Classes

- class gc_summary
- class iterator
- class sync_wrapper
- class timer

Functions

- def _raiseExitNow
- def defer
- def event_loop
- def exit_event_loop
- def run_deferred

Variables

- list deferred_queue = []

  List to hold deferred actions.

- ExitNow = asyncore.ExitNow

9.6.1 Detailed Description

Utilities for event-driven programming.

$Id: async.py 2926 2010-01-04 22:28:34Z sra $

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

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

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

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

9.6.2 Function Documentation

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

Signal handler for event_loop().

De nition at line 264 of le async.py.

9.6.2.2 def rpki.async.defer (thunk)

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

De nition at line 245 of le async.py.

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

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

De nition at line 268 of le async.py.

9.6.2.4 def rpki.async.exit_event_loop ()

Force exit from event_loop().

De nition at line 343 of le async.py.

9.6.2.5 def rpki.async.run_deferred ()

Run deferred actions.

De nition at line 251 of le async.py.

9.6.3 Variable Documentation

9.6.3.1 rpki::async::deferred_queue = [ ]

List to hold deferred actions. We used to do this with the timer queue, but that appears to confuse the garbage collector, and is overengineering for simple deferred actions in any case.

De nition at line 243 of le async.py.

9.6.3.2 rpki::async.ExitNow = asyncore.ExitNow

De nition at line 24 of le async.py.

9.7 Package rpki.con g

Classes

- class parser

9.7.1 Detailed Description

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

$Id: config.py 2926 2010-01-04 22:28:34Z sra $

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

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

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY

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

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

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

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

9.8 Package rpki.exceptions

Classes

- classBadClassNameSyntax
- classBadClientURL
- classBadContactURL
- classBadExtension
- classBadIRDBReply
- classBadIssueResponse
- classBadPKCS10
- classBadPublicationReply
- classBadQuery
- classBadSender
- classBadStatusCode
- classBadURISyntax
- classBSCNotFound
- classBSCNotReady
- classChildNotFound
- classClassNameMismatch
- classClassNameUnknown
- classClientNotFound
- classCMSContentNotSet
- classCMSCRLNotSet
- classCMSVeri cationFailed
- classDBConsistancyError
- classDERObjectConversionError

- classDuplicateObject
- classEmptyPEM
- classEmptyROAPre xList
- classForbiddenURI
- classHandleTranslationError
- classHTTPRequestFailed
- classHTTPSBadVersion
- classHTTPSClientAborted
- classHTTPSUnexpectedState
- classMissingCMSCRL
- classMissingCMSEEcert
- classMultipleTLSEECert
- classMustBePre x
- classNoActiveCA
- classNoCoveringCertForROA
- classNoObjectAtURI
- classNotACerti cateChain
- classNotFound
- classNotImplementedYet
- classNotInDatabase
- classReceivedTLSCACert
- classRPKI_Exception
- classServerShuttingDown
- classSKIMismatch
- classSubprocessError
- classTLSValidationError
- classUnexpectedCMSCerts
- classUnexpectedCMSCRLs
- classUnparsableCMSDER
- classUpstreamError
- classWrongEContentType

9.8.1 Detailed Description

Exception definitions for RPKI modules.

$Id: exceptions.py 2907 2009-12-23 20:48:19Z sra $

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

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

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

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

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

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

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

9.9 Package rpki.https

Classes

- class http_client
- class http_listener
- class http_message
- class http_queue
- class http_request
- class http_response
- class http_server
- class http_stream

Functions

- def build_https_ta_cache
- def client
- def log_method
- def server

Variables

- dictionary client_queues = {}
- debug_http = False
- debug_tls_certs = False
- tuple default_client_timeout = rpki.sundial.timedelta(minutes = 15)

- tuple default_http_version = (1, 0)
- tuple default_server_timeout = rpki.sundial.timedelta(minutes = 20)
- string rpki_content_type = "application/x-rpki"
- want_persistent_client = False
- want_persistent_server = False

9.9.1 Detailed Description

HTTPS utilities, both client and server.

$Id: https.py 2902 2009-12-22 21:57:32Z 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.

9.9.2 Function Documentation

9.9.2.1 def rpki.https.build_https_ta_cache (certs)

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

De nition at line 766 of le https.py.

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

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

De nition at line 707 of le https.py.

9.9.2.3 def rpki.https.log_method (self, msg, logger= rpki.log.debug)

De nition at line 169 of le https.py.

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

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

De nition at line 752 of le https.py.

9.9.3 Variable Documentation

9.9.3.1 dictionary rpki::https.client_queues = {}

De nition at line 705 of le https.py.

9.9.3.2 rpki::https.debug_http = False

De nition at line 45 of le https.py.

9.9.3.3 rpki::https.debug_tls_certs = False

De nition at line 48 of le https.py.

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

De nition at line 58 of le https.py.

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

De nition at line 61 of le https.py.

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

De nition at line 59 of le https.py.

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

De nition at line 39 of le https.py.

9.9.3.8 rpki::https.want_persistent_client = False

De nition at line 51 of le https.py.

9.9.3.9 rpki::https.want_persistent_server = False

De nition at line 52 of le https.py.

9.10 Package rpki.ipaddrs

Classes

- classv4addr
- classv6addr

9.10.1 Detailed Description

Classes to represent IP addresses.

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

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

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

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

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

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

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

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

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

9.11 Package rpki.left_right

Classes

- class bsc_elt
- class child_elt
- class cms_msg
- class data_elt
- class left_right_namespace
- class list_published_objects_elt
- class list_resources_elt
- class list_roa_requests_elt
- class msg
- class parent_elt
- class report_error_elt
- class repository_elt
- class sax_handler
- class self_elt

Variables

- enforce_strict_up_down_xml_sender = False

9.11.1 Detailed Description

RPKI "left-right" protocol.

$Id: left_right.py 2931 2010-01-06 21:03:14Z sra $

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

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

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

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

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

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

9.11.2 Variable Documentation

9.11.2.1 rpki::left_right.enforce_strict_up_down_xml_sender = False

De nition at line 40 of le left_right.py.

9.12 Package rpki.log

Classes

- class logger

Functions

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

Variables

- tuple debug = logger(syslog.LOG_DEBUG)
- enable_trace = False

  Whether call tracing is enabled.

- tuple error = logger(syslog.LOG_ERR)
- tuple info = logger(syslog.LOG_INFO)
- tuple note = logger(syslog.LOG_NOTICE)
- int pid = 0
- string tag = ""
- use_syslog = True

  Whether to use syslog.

- tuple warn = logger(syslog.LOG_WARNING)

9.12.1 Detailed Description

Logging facilities for RPKI libraries.

$Id: log.py 2933 2010-01-07 01:00:17Z sra $

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

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

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

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

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

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

9.12.2 Function Documentation

9.12.2.1 def rpki.log.init (ident = "rpki" , ags = syslog.LOG_PID , facility = syslog.LOG_DAEMON)

Initialize logging system.

De nition at line 51 of le log.py.

9.12.2.2 def rpki.log.set_trace (enable)

Enable or disable call tracing.

De nition at line 63 of le log.py.

9.12.2.3 def rpki.log.trace ()

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

De nition at line 91 of le log.py.

9.12.2.4 def rpki.log.traceback ()

Consolidated backtrace facility with a bit of extra info.

De nition at line 100 of le log.py.

9.12.3 Variable Documentation

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

De nition at line 89 of le log.py.

9.12.3.2 rpki::log::enable_trace = False

Whether call tracing is enabled.
De nition at line 41 of le log.py.

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

De nition at line 85 of le log.py.

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

De nition at line 88 of le log.py.

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

De nition at line 87 of le log.py.

9.12.3.6 int rpki::log.pid = 0

De nition at line 49 of le log.py.

9.12.3.7 string rpki::log.tag = ""

De nition at line 48 of le log.py.

9.12.3.8 rpki::log::use_syslog = True

Whether to use syslog.

De nition at line 46 of le log.py.

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

De nition at line 86 of le log.py.

9.13 Package rpki.manifest

Classes

- class FileAndHash
- class FilesAndHashes
- class Manifest

9.13.1 Detailed Description

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

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

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

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

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

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

9.14 Package rpki.oids

Variables

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

  Mapping table of string names to OIDs.

- dictionary oid2name

  Mapping table of OIDs to conventional string names.

9.14.1 Detailed Description

OID database.

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

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

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

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

9.14.2 Variable Documentation

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

Mapping table of string names to OIDs.

De nition at line 58 of le oids.py.

9.14.2.2 rpki::oids::oid2name

Initial value:

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

Mapping table of OIDs to conventional string names.

De nition at line 24 of le oids.py.

9.15 Package rpki.publication

Classes

- classcerti cate_elt
- classclient_elt
- classcms_msg
- classcon g_elt
- classcontrol_elt
- classcrl_elt
- classmanifest_elt
- classmsg
- classpublication_namespace
- classpublication_object_elt
- classreport_error_elt
- classroa_elt
- classsax_handler

9.15.1 Detailed Description

RPKI "publication" protocol.

$Id: publication.py 2935 2010-01-07 17:23:05Z sra $

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

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

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

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

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

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

9.16 Package rpki.relaxng

Variables

- tuple left_right
  Parsed RelaxNG left_right schema.
- tuple publication
  Parsed RelaxNG publication schema.
- tuple up_down
  Parsed RelaxNG up_down schema.

9.16.1 Variable Documentation

9.16.1.1 rpki::relaxng::left_right

Parsed RelaxNG left_right schema.

De nition at line 7 of le relaxng.py.

9.16.1.2 rpki::relaxng::publication

Parsed RelaxNG publication schema.

De nition at line 1171 of le relaxng.py.

9.16.1.3 rpki::relaxng::up_down

Parsed RelaxNG up_down schema.

De nition at line 917 of le relaxng.py.

9.17 Package rpki.resource_set

Classes

- class resource_bag

- class resource_range
- class resource_range_as
- class resource_range_ip
- class resource_range_ipv4
- class resource_range_ipv6
- class resource_set
- class resource_set_as
- class resource_set_ip
- class resource_set_ipv4
- class resource_set_ipv6
- class roa_pre x
- class roa_pre x_ipv4
- class roa_pre x_ipv6
- class roa_pre x_set
- class roa_pre x_set_ipv4
- class roa_pre x_set_ipv6

Functions

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

Variables

- string inherit_token = "<inherit>"

  Token used to indicate inheritance in read and print syntax.

9.17.1 Detailed Description

Classes dealing with sets of resources.

The basic mechanics of a resource set are the same for any of the resources we handle (ASNs, IPv4 addresses, or IPv6 addresses), so we can provide the same operations on any of them, even though the underlying details vary.

We also provide some basic set operations (union, intersection, etc).

$Id: resource_set.py 2776 2009-09-19 03:26:51Z sra $

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

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

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

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

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

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

9.17.2 Function Documentation

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

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

De nition at line 514 of le resource_set.py.

9.17.2.2 def rpki.resource_set._long2bs(number, addrlen, pre xlen = 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.

De nition at line 526 of le resource_set.py.

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

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

De nition at line 190 of le resource_set.py.

9.17.2.4 def rpki.resource_set.test1t(s1, s2)

De nition at line 884 of le resource_set.py.

9.17.2.5 def rpki.resource_set.test2t(s1, s2)

De nition at line 917 of le resource_set.py.

9.17.3 Variable Documentation

9.17.3.1 rpki::resource_set::inherit_token = "<inherit >"

Token used to indicate inheritance in read and print syntax.

De nition at line 48 of le resource_set.py.

9.18 Package rpki.roa

Classes

- class ROAIPAddress
- class ROAIPAddresses
- class ROAIPAddressFamilies
- class ROAIPAddressFamily
- class RouteOriginAttestation

9.18.1 Detailed Description

ROA (Route Origin Authorization).

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

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

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

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

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

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

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

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

ASID ::= INTEGER

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

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

IPAddress ::= BIT STRING
```

9.19 Package rpki.rpki_engine

Classes

- class ca_detail_obj
- class ca_obj
- class child_cert_obj
- class publication_queue
- class revoked_cert_obj
- class roa_obj
- class rpkid_context

9.19.1 Detailed Description

Global context for rpkid.

$Id: rpki_engine.py 2934 2010-01-07 01:22:04Z 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.

9.20 Package rpki.sql

Classes

- classsession
- classsql_persistent
- classtemplate

9.20.1 Detailed Description

SQL interface code.

$Id: sql.py 2895 2009-12-21 17:17:55Z sra $

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

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

copyright notice and this permission notice appear in all copies.

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

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

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

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

9.21 Package rpki.sundial

Classes

- class datetime
- class timedelta

Functions

- def _cast
- def now
- def test

9.21.1 Detailed Description

Unified RPKI date/time handling, based on the standard Python datetime module.

Module name chosen to sidestep a nightmare of import-related errors that occur with the more obvious module names.

List of arithmetic methods that require result casting was derived by inspection of the datetime module, to wit:

```
>>> import datetime
>>> for t in (datetime.datetime, datetime.timedelta):
...     for k in t.__dict__.keys():
```

```
...     if k.startswith("__"):
...       print "%s.%s()" % (t.__name__, k)
```

$Id: sundial.py 2785 2009-09-25 20:21:53Z sra $

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

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

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

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

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

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

9.21.2 Function Documentation

9.21.2.1 def rpki.sundial._cast (k) [private]

Cast result of arithmetic operations back into correct subtype.

De nition at line 232 of le sundial.py.

9.21.2.2 def rpki.sundial.now ()

Get current timestamp.

De nition at line 50 of le sundial.py.

9.21.2.3 def rpki.sundial.test (t)

De nition at line 244 of le sundial.py.

9.22 Package rpki.up_down

Classes

- class base_elt
- class certi cate_elt
- class class_elt
- class class_response_syntax
- class cms_msg
- class error_response_pdu
- class issue_pdu
- class issue_response_pdu
- class list_pdu
- class list_response_pdu
- class message_pdu
- class multi_uri
- class revoke_pdu
- class revoke_response_pdu
- class revoke_syntax
- class sax_handler

Variables

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

9.22.1 Detailed Description

RPKI "up-down" protocol.

$Id: up_down.py 2935 2010-01-07 17:23:05Z sra $

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

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

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

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

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

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

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

9.22.2 Variable Documentation

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

De nition at line 41 of le up_down.py.

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

De nition at line 39 of le up_down.py.

9.23 Package rpki.x509

Classes

- classCMS_object
- classCRL
- classDeadDrop
- classDER_CMS_object
- classDER_object
- classPEM_converter
- classPKCS10
- classROA

- class RSA
- class RSApublic
- class SignedManifest
- class X509
- class XML_CMS_object

Functions

- def calculate_SKI
- def POWify_OID

9.23.1 Detailed Description

One X.509 implementation to rule them all...

...and in the darkness hide the twisty maze of partially overlapping X.509 support packages in Python.

There are several existing packages, none of which do quite what I need, due to age, lack of documentation, specialization, or lack of foresight on somebody's part (perhaps mine). This module attempts to bring together the functionality I need in a way that hides at least some of the nasty details. This involves a lot of format conversion.

$Id: x509.py 2928 2010-01-05 05:45:35Z sra $

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

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

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

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

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

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

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

9.23.2 Function Documentation

9.23.2.1 def rpki.x509.calculate_SKI (public_key_der)

Calculate the SKI value given the DER representation of a public key, which requires first peeling the ASN.1 wrapper off the key.

De nition at line 51 of le x509.py.

9.23.2.2 def rpki.x509.POWify_OID (oid)

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

De nition at line 692 of le x509.py.

9.24 Package rpki.xml_utils

Classes

- class base_elt
- class data_elt
- class msg
- class sax_handler
- class text_elt

9.24.1 Detailed Description

XML utilities.

$Id: xml_utils.py 2836 2009-10-26 22:31:16Z sra $

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

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

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

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

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

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

9.25 Package rpkid

Functions

- def main

Variables

- string cfg_ le = "rpkid.conf"
- pro le = None

9.25.1 Detailed Description

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

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

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

$Id: rpkid.py 2913 2009-12-28 20:55:38Z sra $

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

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

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

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

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

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

9.25.2 Function Documentation

9.25.2.1 def rpkid.main ()

De nition at line 68 of le rpkid.py.

9.25.3 Variable Documentation

9.25.3.1 rpkid.cfg_ le = "rpkid.conf"

De nition at line 49 of le rpkid.py.

9.25.3.2 rpkid.pro le = None

De nition at line 50 of le rpkid.py.

10 Class Documentation

10.1 async_chat Class Reference

Inherited by rpki.https.http_stream

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

- https.py (2902)

10.2 dispatcher Class Reference

Inherited by rpki.https.http_listener

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

- https.py (2902)

10.3 Exception Class Reference

Inherited by rpki.exceptions.RPKI_Exception

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

- exceptions.py (2907)

10.4 irbe_cli.bsc_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::bsc_elt

Public Member Functions

- def client_query_signing_cert
- def client_query_signing_cert_crl
- def client_reply_decode

Public Attributes

- signing_cert
- signing_cert_crl

Static Public Attributes

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

10.4.1 Detailed Description

De nition at line 189 of le irbe_cli.py.

10.4.2 Member Function Documentation

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

--signing_cert option.

De nition at line 193 of le irbe_cli.py.

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

--signing_cert_crl option.

De nition at line 197 of le irbe_cli.py.

10.4.2.3 def irbe_cli.bsc_elt.client_reply_decode(self)

Reimplemented from irbe_cli.reply_elt_mixin.
De nition at line 201 of le irbe_cli.py.

10.4.3 Member Data Documentation

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

XML attributes and elements that should not be allowed as command line arguments.
Reimplemented from irbe_cli.cmd_elt_mixin.

De nition at line 191 of le irbe_cli.py.

10.4.3.2 irbe_cli.bsc_elt.signing_cert

Reimplemented from rpki.left_right.bsc_elt

De nition at line 195 of le irbe_cli.py.

10.4.3.3 irbe_cli.bsc_elt.signing_cert_crl

Reimplemented from rpki.left_right.bsc_elt

De nition at line 199 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.5 irbe_cli.caller Class Reference

Inherits object.

Public Member Functions

- def __call__
- def __init__

Public Attributes

- client_cert
- client_key
- cms_class
- server_cert
- server_ta
- url

10.5.1 Detailed Description

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

De nition at line 41 of le irbe_cli.py.

10.5.2 Member Function Documentation

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

De nition at line 55 of le irbe_cli.py.

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

De nition at line 47 of le irbe_cli.py.

10.5.3 Member Data Documentation

10.5.3.1 irbe_cli.caller.client_cert

De nition at line 50 of le irbe_cli.py.

10.5.3.2 irbe_cli.caller.client_key

De nition at line 49 of le irbe_cli.py.

10.5.3.3 irbe_cli.caller.cms_class

De nition at line 48 of le irbe_cli.py.

10.5.3.4 irbe_cli.caller.server_cert

De nition at line 52 of le irbe_cli.py.

10.5.3.5 irbe_cli.caller.server_ta

De nition at line 51 of le irbe_cli.py.

10.5.3.6 irbe_cli.caller.url

De nition at line 53 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.6 irbe_cli.certi cate_elt Class Reference

Inheritsirbe_cli::cmd_elt_mixin, andrpki::publication::certi cate_elt

10.6.1 Detailed Description

De nition at line 246 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.7 irbe_cli.child_elt Class Reference

Inheritsirbe_cli::cmd_elt_mixin, andrpki::left_right::child_elt

10.7.1 Detailed Description

De nition at line 211 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.8 irbe_cli.client_elt Class Reference

Inheritsirbe_cli::cmd_elt_mixin, andrpki::publication::client_elt

10.8.1 Detailed Description

De nition at line 243 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.9 irbe_cli.cmd_elt_mixin Class Reference

Inherits irbe_cli::reply_elt_mixin.

Inherited by irbe_cli.bsc_elt, irbe_cli.certi cate_elt, irbe_cli.child_elt, irbe_cli.client_elt, irbe_cli.con g_elt, irbe_cli.crl_elt, irbe_cli.list_published_objects_elt, irbe_cli.manifest_elt, irbe_cli.parent_elt, irbe_cli.repository_elt, irbe_cli.roa_elt, and irbe_cli.self_elt.

Public Member Functions

- def client_getopt
- def client_query_bpki_cert
- def client_query_bpki_cms_cert
- def client_query_bpki_https_cert
- def client_query_cms_glue
- def client_query_glue
- def client_query_https_glue
- def usage

Public Attributes

- bpki_cert
- bpki_cms_cert
- bpki_cms_glue
- bpki_glue
- bpki_https_cert
- bpki_https_glue

Static Public Attributes

- tuple excludes = ()

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

- is_cmd = True

10.9.1 Detailed Description

Protocol mix-in for command line client element PDUs.

De nition at line 105 of le 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.

De nition at line 129 of le 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.

De nition at line 146 of le irbe_cli.py.

10.9.2.3 def irbe_cli.cmd_elt_mixin.client_query_bpki_cms_certs (self, arg)

Special handler for --bpki_cms_cert option.

De nition at line 154 of le 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.

De nition at line 162 of le irbe_cli.py.

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

Special handler for --bpki_cms_glue option.

Definition at line 158 of file irbe_cli.py.

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

Special handler for --bpki_glue option.

Definition at line 150 of file irbe_cli.py.

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

Special handler for --bpki_https_glue option.

Definition at line 166 of file irbe_cli.py.

10.9.2.8 def irbe_cli.cmd_elt_mixin.usage(cls)

Generate usage message for this PDU.

Definition at line 118 of file irbe_cli.py.

10.9.3 Member Data Documentation

10.9.3.1 irbe_cli.cmd_elt_mixin.bpki_cert

Definition at line 148 of file irbe_cli.py.

10.9.3.2 irbe_cli.cmd_elt_mixin.bpki_cms_cert

Definition at line 156 of file irbe_cli.py.

10.9.3.3 irbe_cli.cmd_elt_mixin.bpki_cms_glue

De nition at line 160 of le irbe_cli.py.

10.9.3.4 irbe_cli.cmd_elt_mixin.bpki_glue

De nition at line 152 of le irbe_cli.py.

10.9.3.5 irbe_cli.cmd_elt_mixin.bpki_https_cert

De nition at line 164 of le irbe_cli.py.

10.9.3.6 irbe_cli.cmd_elt_mixin.bpki_https_glue

De nition at line 168 of le irbe_cli.py.

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

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

Reimplemented in irbe_cli.bsc_elt, and irbe_cli.list_published_objects_elt.

De nition at line 115 of le irbe_cli.py.

10.9.3.8 irbe_cli.cmd_elt_mixin.is_cmd = True [static]

Reimplemented from irbe_cli.reply_elt_mixin.

De nition at line 110 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.10 irbe_cli.cmd_msg_mixin Class Reference

Inherits object.

Inherited by irbe_cli.left_right_msg and irbe_cli.publication_msg.

Public Member Functions

- def usage

10.10.1 Detailed Description

Protocol mix-in for command line client message PDUs.

Definition at line 170 of file irbe_cli.py.

10.10.2 Member Function Documentation

10.10.2.1 def irbe_cli.cmd_msg_mixin.usage(cls)

Generate usage message for this PDU.

Definition at line 176 of file irbe_cli.py.

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

- irbe_cli.py (2799)

10.11 irbe_cli.con g_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::con g_elt.

Public Member Functions

- def client_query_bpki_crl

Public Attributes

- bpki_crl

10.11.1 Detailed Description

De nition at line 237 of le irbe_cli.py.

10.11.2 Member Function Documentation

10.11.2.1 def irbe_cli.con g_elt.client_query_bpki_crl (self, arg)

Special handler for --bpki_crl option.

De nition at line 239 of le irbe_cli.py.

10.11.3 Member Data Documentation

10.11.3.1 irbe_cli.con g_elt.bpki_crl

De nition at line 241 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.12 irbe_cli.crl_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::crl_elt.

10.12.1 Detailed Description

De nition at line 249 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.13 irbe_cli.left_right_cms_msg Class Reference

Inherits rpki::left_right::cms_msg

Static Public Attributes

- saxify = left_right_sax_handler.saxify

10.13.1 Detailed Description

De nition at line 232 of le irbe_cli.py.

10.13.2 Member Data Documentation

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

Reimplemented from rpki.left_right.cms_msg.

De nition at line 233 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.14 irbe_cli.left_right_msg Class Reference

Inherits irbe_cli::cmd_msg_mixin, and rpki::left_right::msg.

Static Public Attributes

- tuple pdus

  Dispatch table of PDUs for this protocol.

10.14.1 Detailed Description

De nition at line 224 of le irbe_cli.py.

10.14.2 Member Data Documentation

10.14.2.1 tuple irbe_cli.left_right_msg.pdus [static]

Initial value:

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

                                        list_published_objects_elt, report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented from rpki.left_right.msg.

De nition at line 225 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.15 irbe_cli.left_right_sax_handler Class Reference

Inherits rpki::left_right::sax_handler

Static Public Attributes

- pdu = left_right_msg

10.15.1 Detailed Description

De nition at line 229 of le 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.

De nition at line 230 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.16 irbe_cli.list_published_objects_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::list_published_objects_elt

Static Public Attributes

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

10.16.1 Detailed Description

De nition at line 217 of le irbe_cli.py.

10.16.2 Member Data Documentation

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

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

Reimplemented from irbe_cli.cmd_elt_mixin

De nition at line 219 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.17 irbe_cli.manifest_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::manifest_elt

10.17.1 Detailed Description

De nition at line 252 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.18 irbe_cli.parent_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::parent_elt

10.18.1 Detailed Description

De nition at line 208 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.19 irbe_cli.publication_cms_msg Class Reference

Inherits rpki::publication::cms_msg

Static Public Attributes

- saxify = publication_sax_handler.saxify

10.19.1 Detailed Description

De nition at line 268 of le irbe_cli.py.

10.19.2 Member Data Documentation

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

Reimplemented from rpki.publication.cms_msg

De nition at line 269 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.20 irbe_cli.publication_msg Class Reference

Inherits irbe_cli::cmd_msg_mixin, and rpki::publication::msg

Static Public Attributes

- tuple pdus

  Dispatch table of PDUs for this protocol.

10.20.1 Detailed Description

De nition at line 261 of le irbe_cli.py.

10.20.2 Member Data Documentation

10.20.2.1 tuple irbe_cli.publication_msg.pdus [static]

Initial value:

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

Dispatch table of PDUs for this protocol.

Reimplemented from rpki.publication.msg

De nition at line 262 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.21 irbe_cli.publication_sax_handler Class Reference

Inherits rpki::publication::sax_handler

Static Public Attributes

- pdu = publication_msg

10.21.1 Detailed Description

De nition at line 265 of le irbe_cli.py.

10.21.2 Member Data Documentation

10.21.2.1 irbe_cli.publication_sax_handler.pdu = publication_msg [static]

Reimplemented from rpki.publication.sax_handler

De nition at line 266 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.22 irbe_cli.reply_elt_mixin Class Reference

Inherits object.

Inherited by irbe_cli.cmd_elt_mixin, irbe_cli.report_error_elt, and irbe_cli.report_error_elt.

Public Member Functions

- def client_reply_decode
- def client_reply_show

Static Public Attributes

- is_cmd = False

10.22.1 Detailed Description

Protocol mix-in for printout of reply PDUs.

Definition at line 89 of file irbe_cli.py.

10.22.2 Member Function Documentation

10.22.2.1 def irbe_cli.reply_elt_mixin.client_reply_decode(self)

Reimplemented in irbe_cli.bsc_elt.

Definition at line 96 of file irbe_cli.py.

10.22.2.2 def irbe_cli.reply_elt_mixin.client_reply_show(self)

Definition at line 99 of file irbe_cli.py.

10.22.3 Member Data Documentation

10.22.3.1 irbe_cli.reply_elt_mixin.is_cmd = False [static]

Reimplemented in irbe_cli.cmd_elt_mixin.

De nition at line 94 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.23 irbe_cli.report_error_elt Class Reference

Inherits irbe_cli::reply_elt_mixin, rpki::publication::report_error_elt, irbe_cli::reply_elt_mixin, and rpki::left_right::report_error_elt.

10.23.1 Detailed Description

De nition at line 221 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.24 irbe_cli.repository_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::left_right::repository_elt.

10.24.1 Detailed Description

De nition at line 214 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.25 irbe_cli.roa_elt Class Reference

Inherits irbe_cli::cmd_elt_mixin, and rpki::publication::roa_elt.

10.25.1 Detailed Description

De nition at line 255 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.26 irbe_cli.self_elt Class Reference

Inheritsirbe_cli::cmd_elt_mixin, andrpki::left_right::self_elt.

10.26.1 Detailed Description

De nition at line 186 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.27 irbe_cli.UsageWrapper Class Reference

Inheritstextwrap::TextWrapper.

Public Member Functions

- def __call__

10.27.1 Detailed Description

Call interface around Python textwrap.Textwrapper class.

De nition at line 78 of le irbe_cli.py.

10.27.2 Member Function Documentation

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

Format arguments, with TextWrapper indentation.

De nition at line 83 of le irbe_cli.py.

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

- irbe_cli.py (2799)

10.28 long Class Reference

Inherited by rpki.ipaddrs.v4addr, and rpki.ipaddrs.v6addr.

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

- ipaddrs.py (2424)

10.29 object Class Reference

Inherited by irbe_cli.caller, irbe_cli.cmd_msg_mixin, irbe_cli.reply_elt_mixin, pubd.pubd_context, rpki.async.gc_summary, rpki.async.iterator, rpki.async.sync_wrapper, rpki.async.timer, rpki.con g.parser, rpki.https.http_message, rpki.https.http_queue, rpki.left_right.left_right_namespace, rpki.log.logger, rpki.publication.publication_namespace, rpki.resource_set.resource_bag, rpki.resource_set.resource_range, rpki.resource_set.roa_pre x, rpki.rpki_engine.publication_queue, rpki.rpki_engine.rpkid_context, rpki.sql.session, rpki.sql.sql_persistent, rpki.sql.template, rpki.up_down.base_elt, rpki.x509.DeadDrop, rpki.x509.DER_object, rpki.x509.PEM_converter, and rpki.xml_utils.base_elt.

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

- x509.py (2928)

10.30 pubd.pubd_context Class Reference

Inherits object.

Public Member Functions

- def __init__
- def build_https_ta_cache
- def clear_https_ta_cache
- def client_handler
- def control_handler
- def handler_common

Public Attributes

- bpki_ta
- https_server_host
- https_server_port
- irbe_cert
- pubd_cert
- pubd_key
- publication_base
- sql

Static Public Attributes

- tuple client_url_regexp = re.compile("/client/([-A-Z0-9_/]+)$", re.I)
- https_ta_cache = None

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

10.30.1 Detailed Description

A container for various pubd parameters.

De nition at line 46 of le pubd.py.

10.30.2 Member Function Documentation

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

De nition at line 51 of le pubd.py.

10.30.2.2 def pubd.pubd_context.build_https_ta_cache(self)

Build dynamic TLS trust anchors.

De nition at line 138 of le pubd.py.

10.30.2.3 def pubd.pubd_context.clear_https_ta_cache(self)

Clear dynamic TLS trust anchors.

De nition at line 130 of le pubd.py.

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

Process one PDU from a client.

De nition at line 98 of le pubd.py.

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

Process one PDU from the IRBE.

De nition at line 78 of le pubd.py.

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

Common PDU handler code.

De nition at line 65 of le pubd.py.

10.30.3 Member Data Documentation

10.30.3.1 pubd.pubd_context.bpki_ta

De nition at line 55 of le pubd.py.

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

De nition at line 96 of le pubd.py.

10.30.3.3 pubd.pubd_context.https_server_host

De nition at line 60 of le pubd.py.

10.30.3.4 pubd.pubd_context.https_server_port

De nition at line 61 of le pubd.py.

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

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

De nition at line 128 of le pubd.py.

10.30.3.6 pubd.pubd_context.irbe_cert

De nition at line 56 of le pubd.py.

10.30.3.7 pubd.pubd_context.pubd_cert

De nition at line 57 of le pubd.py.

10.30.3.8 pubd.pubd_context.pubd_key

De nition at line 58 of le pubd.py.

10.30.3.9 pubd.pubd_context.publication_base

De nition at line 63 of le pubd.py.

10.30.3.10 pubd.pubd_context.sql

De nition at line 53 of le pubd.py.

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

- pubd.py (2913)

10.31 datetime Class Reference

Inherited byrpki.sundial.datetime

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

- sundial.py (2785)

10.32 timedelta Class Reference

Inherited byrpki.sundial.timedelta

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

- sundial.py (2785)

10.33 rootd.cms_msg Class Reference

Inheritsrpki::up_down::cms_msg

Static Public Attributes

- saxify = sax_handler.saxify

10.33.1 Detailed Description

De nition at line 235 of le rootd.py.

10.33.2 Member Data Documentation

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

Reimplemented from rpki.up_down.cms_msg.

De nition at line 236 of le rootd.py.

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

- rootd.py (2913)

10.34 rootd.issue_pdu Class Reference

Inherits rpki::up_down::issue_pdu.

Public Member Functions

- def serve_pdu

10.34.1 Detailed Description

De nition at line 194 of le rootd.py.

10.34.2 Member Function Documentation

10.34.2.1 def rootd.issue_pdu.serve_pdu(self, q_msg, r_msg, child, callback, errback)

Serve one issue request PDU.

Reimplemented from rpki.up_down.issue_pdu.

De nition at line 195 of le rootd.py.

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

- rootd.py (2913)

10.35 rootd.list_pdu Class Reference

Inherits rpki::up_down::list_pdu.

Public Member Functions

- def serve_pdu

10.35.1 Detailed Description

De nition at line 188 of le rootd.py.

10.35.2 Member Function Documentation

10.35.2.1 def rootd.list_pdu.serve_pdu(self, q_msg, r_msg, child, callback, errback)

Serve one "list" PDU.

Reimplemented from rpki.up_down.list_pdu.

De nition at line 189 of le rootd.py.

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

- rootd.py (2913)

10.36 rootd.message_pdu Class Reference

Inherits rpki::up_down::message_pdu.

Public Member Functions

- def log_query

Static Public Attributes

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

10.36.1 Detailed Description

De nition at line 213 of le rootd.py.

10.36.2 Member Function Documentation

10.36.2.1 def rootd.message_pdu.log_query(self, child)

Log query we're handling.

Reimplemented from rpki.up_down.message_pdu.

De nition at line 226 of le rootd.py.

10.36.3 Member Data Documentation

10.36.3.1 dictionary rootd.message_pdu.name2type [static]

Initial value:

```
{
    "list"                      : list_pdu,
    "list_response"     : rpki.up_down.list_response_pdu,
    "issue"                     : issue_pdu,
    "issue_response"    : rpki.up_down.issue_response_pdu,
    "revoke"                    : revoke_pdu,
    "revoke_response" : rpki.up_down.revoke_response_pdu,
    "error_response"    : rpki.up_down.error_response_pdu }
```

Reimplemented from rpki.up_down.message_pdu.

De nition at line 215 of le rootd.py.

10.36.3.2 tuple rootd.message_pdu.type2name = dict((v, k) for k, v in name2type.items()) [static]

Reimplemented from rpki.up_down.message_pdu.

De nition at line 224 of le rootd.py.

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

- rootd.py (2913)

10.37 rootd.revoke_pdu Class Reference

Inherits rpki::up_down::revoke_pdu

Public Member Functions

- def serve_pdu

10.37.1 Detailed Description

De nition at line 201 of le rootd.py.

10.37.2 Member Function Documentation

10.37.2.1 def rootd.revoke_pdu.serve_pdu(self, q_msg, r_msg, child, cb, eb)

Serve one revoke request PDU.

Reimplemented from rpki.up_down.revoke_pdu

De nition at line 202 of le rootd.py.

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

- rootd.py (2913)

10.38 rootd.sax_handler Class Reference

Inherits rpki::up_down::sax_handler.

Static Public Attributes

- pdu = message_pdu

10.38.1 Detailed Description

De nition at line 232 of le rootd.py.

10.38.2 Member Data Documentation

10.38.2.1 rootd.sax_handler.pdu = message_pdu [static]

Reimplemented from rpki.up_down.sax_handler.

De nition at line 233 of le rootd.py.

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

- rootd.py (2913)

10.39 rpki.async.gc_summary Class Reference

Inherits object.

Public Member Functions

- def __init__
- def handler

Public Attributes

- interval
- timer

10.39.1 Detailed Description

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

De nition at line 347 of le async.py.

10.39.2 Member Function Documentation

10.39.2.1 def rpki.async.gc_summary.__init__(self, interval)

De nition at line 352 of le async.py.

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

De nition at line 359 of le async.py.

10.39.3 Member Data Documentation

10.39.3.1 rpki.async.gc_summary.interval

De nition at line 355 of le async.py.

10.39.3.2 rpki.async.gc_summary.timer

De nition at line 356 of le async.py.

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

- async.py (2926)

10.40 rpki.async.iterator Class Reference

Inheritsobject

Public Member Functions

- def__call__
- def__init__
- def__repr__
- defdoit
- defignore

Public Attributes

- caller_function
- done_callback
- item_callback
- iterator
- unwind_stack

10.40.1 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.

De nition at line 26 of le async.py.

10.40.2 Member Function Documentation

10.40.2.1 def rpki.async.iterator.__call__ (self)

De nition at line 64 of le async.py.

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

De nition at line 45 of le async.py.

10.40.2.3 def rpki.async.iterator.__repr__ (self)

De nition at line 59 of le async.py.

10.40.2.4 def rpki.async.iterator.doit (self)

De nition at line 70 of le async.py.

10.40.2.5 def rpki.async.iterator.ignore (self, ignored)

De nition at line 77 of le async.py.

10.40.3 Member Data Documentation

10.40.3.1 rpki.async.iterator.caller_function

De nition at line 48 of le async.py.

10.40.3.2 rpki.async.iterator.done_callback

De nition at line 47 of le async.py.

10.40.3.3 rpki.async.iterator.item_callback

De nition at line 46 of le async.py.

10.40.3.4 rpki.async.iterator.iterator

De nition at line 51 of le async.py.

10.40.3.5 rpki.async.iterator.unwind_stack

De nition at line 49 of le async.py.

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

- async.py (2926)

10.41 rpki.async.sync_wrapper Class Reference

Inheritsobject

Public Member Functions

- def __call__
- def __init__

- def cb
- def eb

Public Attributes

- func

Static Public Attributes

- err = None
- res = None

10.41.1 Detailed Description

Synchronous wrapper around asynchronous functions. Running in asynchronous mode at all times makes sense for event-driven daemons, but is kind of tedious for simple scripts, hence this wrapper.

The wrapped function should take at least two arguments: a callback function and an errback function. If any arguments are passed to the wrapper, they will be passed as additional arguments to the wrapped function.

De nition at line 300 of le async.py.

10.41.2 Member Function Documentation

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

De nition at line 326 of le async.py.

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

De nition at line 315 of le async.py.

10.41.2.3 def rpki.async.sync_wrapper.cb(self, res = None)

De nition at line 318 of le async.py.

10.41.2.4 def rpki.async.sync_wrapper.ebs(self, err)

De nition at line 322 of le async.py.

10.41.3 Member Data Documentation

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

De nition at line 313 of le async.py.

10.41.3.2 rpki.async.sync_wrapper.func

De nition at line 316 of le async.py.

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

De nition at line 312 of le async.py.

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

- async.py (2926)

10.42 rpki.async.timer Class Reference

Inherits object.

Public Member Functions

- def __cmp__
- def __del__
- def __init__
- def __repr__
- def cancel
- def clear
- def errback
- def handler

- def is_set
- def runq
- def seconds_until_wakeup
- def set
- def set_errback
- def set_handler
- def trace

Public Attributes

- errback
- handler
- when

Static Public Attributes

- gc_debug = False

  Verbose chatter about timers states and garbage collection.

- list queue = []

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

- run_debug = False

  Verbose chatter about timers being run.

10.42.1 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 wakup 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 explict handler turns out to be very convenient when combined with bound methods to other objects.

De nition at line 80 of le async.py.

10.42.2 Member Function Documentation

10.42.2.1 def rpki.async.timer.__cmp__(self, other)

De nition at line 138 of le async.py.

10.42.2.2 def rpki.async.timer.__del__(self)

De nition at line 142 of le async.py.

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

De nition at line 107 of le async.py.

10.42.2.4 def rpki.async.timer.__repr__(self)

De nition at line 204 of le async.py.

10.42.2.5 def rpki.async.timer.cancel(self)

Cancel a timer, if it was set.

De nition at line 145 of le async.py.

10.42.2.6 def rpki.async.timer.clear(cls)

Cancel every timer on the queue. We could just throw away the queue content, but this way we can notify subclasses that provide their own cancel() method.

De nition at line 229 of le async.py.

10.42.2.7 def rpki.async.timer.errback (self, e)

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

De nition at line 176 of le async.py.

10.42.2.8 def rpki.async.timer.handler (self)

Handle a timer that has expired. This must either be overriden by a subclass or set dynamically by set_handler().

De nition at line 159 of le async.py.

10.42.2.9 def rpki.async.timer.is_set (self)

Test whether this timer is currently set.

De nition at line 155 of le async.py.

10.42.2.10 def rpki.async.timer.runq (cls)

Run the timer queue: for each timer whose call time has passed, pull the timer off the queue and call its handler() method.

De nition at line 188 of le async.py.

10.42.2.11 def rpki.async.timer.seconds_until_wakeup (cls)

Calculate delay until next timer expires, or None if no timers are set and we should wait indefinitely. Rounds up to avoid spinning in select() or poll(). We could calculate fractional seconds in the right units instead, but select() and poll() don't even take the same units (argh!), and we're not doing anything that hair-triggered, so rounding up is simplest.

De nition at line 208 of le async.py.

10.42.2.12 def rpki.async.timer.set(self, when)

Set a timer. Argument can be a datetime, to specify an absolute time, or a timedelta, to specify an offset time.

Definition at line 123 of file async.py.

10.42.2.13 def rpki.async.timer.set_errback(self, errback)

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

Definition at line 183 of file async.py.

10.42.2.14 def rpki.async.timer.set_handler(self, handler)

Set timer's expiration handler. This is an alternative to subclassing the timer class, and may be easier to use when integrating timers into other classes (eg, the handler can be a bound method to an object in a class representing a network connection).

Definition at line 166 of file async.py.

10.42.2.15 def rpki.async.timer.trace(self, msg)

Debug logging.

Definition at line 115 of file async.py.

10.42.3 Member Data Documentation

10.42.3.1 rpki.async.timer.errback

Definition at line 185 of file async.py.

10.42.3.2 rpki::async.timer::gc_debug = False [static]

Verbose chatter about timers states and garbage collection.

De nition at line 97 of le async.py.

10.42.3.3 rpki.async.timer.handler

De nition at line 174 of le async.py.

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

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

De nition at line 105 of le async.py.

10.42.3.5 rpki::async.timer::run_debug = False [static]

Verbose chatter about timers being run.

De nition at line 101 of le async.py.

10.42.3.6 rpki.async.timer.when

De nition at line 112 of le async.py.

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

- async.py (2926)

10.43 rpki.con g.parser Class Reference

Inheritsobject

Public Member Functions

- def __init__
- def get
- def getboolean
- def getint
- def has_option
- def has_section
- def multiget
- def set_global_ ags

Public Attributes

- cfg
- default_section
- lename

Private Member Functions

- def _get_wrapper

10.43.1 Detailed Description

Extensions to stock Python ConfigParser:

Read config file and set default section while initializing parser object.

Support for OpenSSL-style subscripted options.

get-methods with default values and default section name.

De nition at line 38 of le con g.py.

10.43.2 Member Function Documentation

10.43.2.1 def rpki.con g.parser.__init__ (self, lename, section= None, allow_missing= False)

Initialize this parser.

De nition at line 49 of le con g.py.

10.43.2.2 def rpki.con g.parser._get_wrapper (self, method, section, option, default) [private]

Wrapper method to add default value and default section support to ConfigParser methods.

De nition at line 98 of le con g.py.

10.43.2.3 def rpki.con g.parser.get (self, option, default = None, section= None)

Get an option, perhaps with a default value.

De nition at line 111 of le con g.py.

10.43.2.4 def rpki.con g.parser.getboolean (self, option, default = None, section= None)

Get a boolean option, perhaps with a default value.

De nition at line 117 of le con g.py.

10.43.2.5 def rpki.con g.parser.getint (self, option, default = None, section= None)

Get an integer option, perhaps with a default value.

De nition at line 123 of le con g.py.

10.43.2.6 def rpki.con g.parser.has_option (self, option, section= None)

Test whether an option exists.

De nition at line 70 of le con g.py.

10.43.2.7 def rpki.con g.parser.has_section(self, section)

Test whether a section exists.

De nition at line 63 of le con g.py.

10.43.2.8 def rpki.con g.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.

De nition at line 79 of le con g.py.

10.43.2.9 def rpki.con g.parser.set_global_ ags (self)

Consolidated control for all the little global control flags scattered through the libraries. This isn't a particularly good place for this function to live, but it has to live somewhere and making it a method of the config parser from which it gets all of its data is less silly than the available alternatives.

De nition at line 129 of le con g.py.

10.43.3 Member Data Documentation

10.43.3.1 rpki.con g.parser.cfg

De nition at line 55 of le con g.py.

10.43.3.2 rpki.con g.parser.default_section

De nition at line 61 of le con g.py.

10.43.3.3 rpki.con g.parser. lename

De nition at line 54 of le con g.py.

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

- con g.py (2926)

10.44 rpki.exceptions.BadClassNameSyntax Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.44.1 Detailed Description

Illegal syntax for a class_name.

De nition at line 92 of le exceptions.py.

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

- exceptions.py (2907)

10.45 rpki.exceptions.BadClientURL Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.45.1 Detailed Description

URL given to HTTPS client does not match profile.

De nition at line 232 of le exceptions.py.

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

- exceptions.py (2907)

10.46 rpki.exceptions.BadContactURL Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.46.1 Detailed Description

Error trying to parse contact URL.

De nition at line 87 of le exceptions.py.

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

- exceptions.py (2907)

10.47 rpki.exceptions.BadExtension Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.47.1 Detailed Description

Forbidden X.509 extension.

De nition at line 242 of le exceptions.py.

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

- exceptions.py (2907)

10.48 rpki.exceptions.BadIRDBReply Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.48.1 Detailed Description

Unexpected reply to IRDB query.

De nition at line 152 of le exceptions.py.

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

- exceptions.py (2907)

10.49 rpki.exceptions.BadIssueResponse Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.49.1 Detailed Description

issue_response PDU with wrong number of classes or certificates.

De nition at line 97 of le exceptions.py.

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

- exceptions.py (2907)

10.50 rpki.exceptions.BadPKCS10 Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.50.1 Detailed Description

Bad PKCS #10 object.

De nition at line 107 of le exceptions.py.

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

- exceptions.py (2907)

10.51 rpki.exceptions.BadPublicationReply Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.51.1 Detailed Description

Unexpected reply to publication query.

De nition at line 257 of le exceptions.py.

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

- exceptions.py (2907)

10.52 rpki.exceptions.BadQuery Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.52.1 Detailed Description

Unexpected protocol query.

De nition at line 55 of le exceptions.py.

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

- exceptions.py (2907)

10.53 rpki.exceptions.BadSender Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.53.1 Detailed Description

Unexpected XML sender value.

De nition at line 127 of le exceptions.py.

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

- exceptions.py (2907)

10.54 rpki.exceptions.BadStatusCode Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.54.1 Detailed Description

Unrecognized protocol status code.

De nition at line 50 of le exceptions.py.

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

- exceptions.py (2907)

10.55 rpki.exceptions.BadURISyntax Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.55.1 Detailed Description

Illegal syntax for a URI.

De nition at line 45 of le exceptions.py.

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

- exceptions.py (2907)

10.56 rpki.exceptions.BSCNotFound Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.56.1 Detailed Description

Could not find specified BSC in database.

De nition at line 122 of le exceptions.py.

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

- exceptions.py (2907)

10.57 rpki.exceptions.BSCNotReady Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.57.1 Detailed Description

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

De nition at line 277 of le exceptions.py.

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

- exceptions.py (2907)

10.58 rpki.exceptions.ChildNotFound Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.58.1 Detailed Description

Could not find specified child in database.

De nition at line 117 of le exceptions.py.

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

- exceptions.py (2907)

10.59 rpki.exceptions.ClassNameMismatch Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.59.1 Detailed Description

class_name does not match child context.

De nition at line 132 of le exceptions.py.

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

- exceptions.py (2907)

10.60 rpki.exceptions.ClassNameUnknown Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.60.1 Detailed Description

Unknown class_name.

De nition at line 137 of le exceptions.py.

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

- exceptions.py (2907)

10.61 rpki.exceptions.ClientNotFound Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.61.1 Detailed Description

Could not find specified client in database.

De nition at line 237 of le exceptions.py.

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

- exceptions.py (2907)

10.62 rpki.exceptions.CMSContentNotSet Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.62.1 Detailed Description

Inner content of a CMS_object has not been set. If object is known to be valid, the .extract() method should be able to set the content; otherwise, only the .verify() method (which checks signatures) is safe.

De nition at line 302 of le exceptions.py.

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

- exceptions.py (2907)

10.63 rpki.exceptions.CMSCRLNotSet Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.63.1 Detailed Description

CMS CRL has not been configured.

De nition at line 217 of le exceptions.py.

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

- exceptions.py (2907)

10.64 rpki.exceptions.CMSVeri cationFailed Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.64.1 Detailed Description

Verification of a CMS message failed.

De nition at line 66 of le exceptions.py.

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

- exceptions.py (2907)

10.65 rpki.exceptions.DBConsistancyError Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.65.1 Detailed Description

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

De nition at line 60 of le exceptions.py.

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

- exceptions.py (2907)

10.66 rpki.exceptions.DERObjectConversionError Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.66.1 Detailed Description

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

De nition at line 76 of le exceptions.py.

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

- exceptions.py (2907)

10.67 rpki.exceptions.DuplicateObject Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.67.1 Detailed Description

Attempt to create an object that already exists.

De nition at line 262 of le exceptions.py.

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

- exceptions.py (2907)

10.68 rpki.exceptions.EmptyPEM Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.68.1 Detailed Description

Couldn't find PEM block to convert.

De nition at line 187 of le exceptions.py.

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

- exceptions.py (2907)

10.69 rpki.exceptions.EmptyROAPre xList Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.69.1 Detailed Description

Can't create ROA with an empty prefix list.

De nition at line 267 of le exceptions.py.

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

- exceptions.py (2907)

10.70 rpki.exceptions.ForbiddenURI Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.70.1 Detailed Description

Forbidden URI, does not start with correct base URI.

De nition at line 247 of le exceptions.py.

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

- exceptions.py (2907)

10.71 rpki.exceptions.HandleTranslationError Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.71.1 Detailed Description

Internal error translating protocol handle -> SQL id.

De nition at line 292 of le exceptions.py.

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

- exceptions.py (2907)

10.72 rpki.exceptions.HTTPRequestFailed Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.72.1 Detailed Description

HTTP request failed.

De nition at line 71 of le exceptions.py.

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

- exceptions.py (2907)

10.73 rpki.exceptions.HTTPSBadVersion Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.73.1 Detailed Description

HTTPS couldn't parse HTTP version.

De nition at line 287 of le exceptions.py.

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

- exceptions.py (2907)

10.74 rpki.exceptions.HTTPSClientAborted Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.74.1 Detailed Description

HTTPS client connection closed while in request-sent state.

De nition at line 252 of le exceptions.py.

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

- exceptions.py (2907)

10.75 rpki.exceptions.HTTPSUnexpectedState Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.75.1 Detailed Description

HTTPS event occurred in an unexpected state.

De nition at line 282 of le exceptions.py.

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

- exceptions.py (2907)

10.76 rpki.exceptions.MissingCMSCRL Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.76.1 Detailed Description

Didn't receive CMS CRL when expecting one.

De nition at line 207 of le exceptions.py.

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

- exceptions.py (2907)

10.77 rpki.exceptions.MissingCMSEEcert Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.77.1 Detailed Description

Didn't receive CMS EE cert when expecting one.

De nition at line 202 of le exceptions.py.

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

- exceptions.py (2907)

10.78 rpki.exceptions.MultipleTLSEECert Class Reference

Inheritsrpki::exceptions::TLSValidationError

10.78.1 Detailed Description

Received more than one TLS EE certificate.

De nition at line 172 of le exceptions.py.

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

- exceptions.py (2907)

10.79 rpki.exceptions.MustBePre x Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.79.1 Detailed Description

Resource range cannot be expressed as a prefix.

De nition at line 162 of le exceptions.py.

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

- exceptions.py (2907)

10.80 rpki.exceptions.NoActiveCA Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.80.1 Detailed Description

No active ca_detail for specified class.

De nition at line 227 of le exceptions.py.

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

- exceptions.py (2907)

10.81 rpki.exceptions.NoCoveringCertForROA Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.81.1 Detailed Description

Couldn't find a covering certificate to generate ROA.

De nition at line 272 of le exceptions.py.

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

- exceptions.py (2907)

10.82 rpki.exceptions.NoObjectAtURI Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.82.1 Detailed Description

No object published at specified URI.

De nition at line 297 of le exceptions.py.

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

- exceptions.py (2907)

10.83 rpki.exceptions.NotACerti cateChain Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.83.1 Detailed Description

Certificates don't form a proper chain.

De nition at line 82 of le exceptions.py.

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

- exceptions.py (2907)

10.84 rpki.exceptions.NotFound Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.84.1 Detailed Description

Object not found in database.

De nition at line 157 of le exceptions.py.

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

- exceptions.py (2907)

10.85 rpki.exceptions.NotImplementedYet Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.85.1 Detailed Description

Internal error -- not implemented yet.

De nition at line 102 of le exceptions.py.

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

- exceptions.py (2907)

10.86 rpki.exceptions.NotInDatabase Class Reference

Inherits rpki::exceptions::RPKI_Exception.

10.86.1 Detailed Description

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

De nition at line 40 of le exceptions.py.

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

- exceptions.py (2907)

10.87 rpki.exceptions.ReceivedTLSCACert Class Reference

Inherits rpki::exceptions::TLSValidationError.

10.87.1 Detailed Description

Received CA certificate via TLS.

De nition at line 177 of le exceptions.py.

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

- exceptions.py (2907)

10.88 rpki.exceptions.RPKI_Exception Class Reference

Inherits Exception.

Inherited by rpki.exceptions.BadClassNameSyntax, rpki.exceptions.BadClientURL, rpki.exceptions.BadContactURL, rpki.exceptions.BadExtension.

rpki.exceptions.BadIRDBReply, rpki.exceptions.BadIssueResponse, rpki.exceptions.BadPKCS10, rpki.exceptions.BadPublicationReply, rpki.exceptions.BadQuery, rpki.exceptions.BadSender, rpki.exceptions.BadStatusCode, rpki.exceptions.BadURISyntax, rpki.exceptions.BSCNotFound, rpki.exceptions.BSCNotReady, rpki.exceptions.ChildNotFound, rpki.exceptions.ClassNameMismatch, rpki.exceptions.ClassNameUnknown, rpki.exceptions.ClientNotFound, rpki.exceptions.CMSContentNotSet, rpki.exceptions.CMSCRLNotSet, rpki.exceptions.CMSVeri cationFailed, rpki.exceptions.DBConsistancyError, rpki.exceptions.DERObjectConversionError, rpki.exceptions.DuplicateObject, rpki.exceptions.EmptyPEM, rpki.exceptions.EmptyROAPre xList, rpki.exceptions.ForbiddenURI, rpki.exceptions.HandleTranslationError, rpki.exceptions.HTTPRequestFailed, rpki.exceptions.HTTPSBadVersion, rpki.exceptions.HTTPSClientAborted, rpki.exceptions.HTTPSUnexpectedState, rpki.exceptions.MissingCMSCRL, rpki.exceptions.MissingCMSEEcert, rpki.exceptions.MustBePre x, rpki.exceptions.NoActiveCA, rpki.exceptions.NoCoveringCertForROA, rpki.exceptions.NoObjectAtURI, rpki.exceptions.NotACerti cateChain, 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.

10.88.1 Detailed Description

Base class for RPKI exceptions.

De nition at line 35 of le exceptions.py.

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

- exceptions.py (2907)

10.89 rpki.exceptions.ServerShuttingDown Class Reference

Inherits rpki::exceptions::RPKI_Exception.

10.89.1 Detailed Description

Server is shutting down.

De nition at line 222 of le exceptions.py.

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

- exceptions.py (2907)

10.90 rpki.exceptions.SKIMismatch Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.90.1 Detailed Description

SKI value in response does not match request.

De nition at line 142 of le exceptions.py.

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

- exceptions.py (2907)

10.91 rpki.exceptions.SubprocessError Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.91.1 Detailed Description

Subprocess returned unexpected error.

De nition at line 147 of le exceptions.py.

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

- exceptions.py (2907)

10.92 rpki.exceptions.TLSValidationError Class Reference

Inheritsrpki::exceptions::RPKI_Exception

Inherited by rpki.exceptions.MultipleTLSEECert and rpki.exceptions.ReceivedTLSCACert

10.92.1 Detailed Description

TLS certificate validation error.

De nition at line 167 of le exceptions.py.

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

- exceptions.py (2907)

10.93 rpki.exceptions.UnexpectedCMSCerts Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.93.1 Detailed Description

Received CMS certs when not expecting any.

De nition at line 192 of le exceptions.py.

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

- exceptions.py (2907)

10.94 rpki.exceptions.UnexpectedCMSCRLs Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.94.1 Detailed Description

Received CMS CRLs when not expecting any.

De nition at line 197 of le exceptions.py.

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

- exceptions.py (2907)

10.95 rpki.exceptions.UnparsableCMSDER Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.95.1 Detailed Description

Alleged CMS DER wasn't parsable.

De nition at line 212 of le exceptions.py.

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

- exceptions.py (2907)

10.96 rpki.exceptions.UpstreamError Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.96.1 Detailed Description

Received an error from upstream.

De nition at line 112 of le exceptions.py.

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

- exceptions.py (2907)

10.97 rpki.exceptions.WrongEContentType Class Reference

Inheritsrpki::exceptions::RPKI_Exception

10.97.1 Detailed Description

Received wrong CMS eContentType.

De nition at line 182 of le exceptions.py.

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

- exceptions.py (2907)

10.98 rpki.https.http_client Class Reference

Inheritsrpki::https::http_stream

Public Member Functions

- def __init__
- def handle_close

- def handle_connect
- def handle_error
- def handle_message
- def handle_no_content_length
- def handle_timeout
- def send_request
- def set_state
- def start
- def tls_connect

Public Attributes

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

Static Public Attributes

- parse_type = http_response
- timeout = default_client_timeout

10.98.1 Detailed Description

De nition at line 519 of le https.py.

10.98.2 Member Function Documentation

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

De nition at line 525 of le https.py.

10.98.2.2 def rpki.https.http_client.handle_close(self)

Reimplemented from rpki.https.http_stream

De nition at line 614 of le https.py.

10.98.2.3 def rpki.https.http_client.handle_connect(self)

De nition at line 546 of le https.py.

10.98.2.4 def rpki.https.http_client.handle_error(self)

Reimplemented from rpki.https.http_stream

De nition at line 629 of le https.py.

10.98.2.5 def rpki.https.http_client.handle_messages(self)

De nition at line 587 of le https.py.

10.98.2.6 def rpki.https.http_client.handle_no_content_length(self)

De nition at line 576 of le https.py.

10.98.2.7 def rpki.https.http_client.handle_timeout(self)

Reimplemented from rpki.https.http_stream

De nition at line 623 of le https.py.

10.98.2.8 def rpki.https.http_client.send_request(self, msg)

De nition at line 579 of le https.py.

10.98.2.9 def rpki.https.http_client.set_state (self, state)

De nition at line 572 of le https.py.

10.98.2.10 def rpki.https.http_client.start (self)

De nition at line 537 of le https.py.

10.98.2.11 def rpki.https.http_client.tls_connect (self)

De nition at line 560 of le https.py.

10.98.3 Member Data Documentation

10.98.3.1 rpki.https.http_client.cert

De nition at line 533 of le https.py.

10.98.3.2 rpki.https.http_client.expect_close

De nition at line 532 of le https.py.

10.98.3.3 rpki.https.http_client.hostport

De nition at line 530 of le https.py.

10.98.3.4 rpki.https.http_client.key

De nition at line 534 of le https.py.

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

De nition at line 521 of le https.py.

10.98.3.6 rpki.https.http_client.queue

De nition at line 529 of le https.py.

10.98.3.7 rpki.https.http_client.retry_read

Reimplemented from rpki.https.http_stream.

De nition at line 564 of le https.py.

10.98.3.8 rpki.https.http_client.retry_write

Reimplemented from rpki.https.http_stream.

De nition at line 566 of le https.py.

10.98.3.9 rpki.https.http_client.state

De nition at line 531 of le https.py.

10.98.3.10 rpki.https.http_client.ta

De nition at line 535 of le https.py.

10.98.3.11 rpki.https.http_client.timeout = default_client_timeout [static]

De nition at line 523 of le https.py.

10.98.3.12 rpki.https.http_client.tls

Reimplemented from rpki.https.http_stream.

De nition at line 548 of le https.py.

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

- https.py (2902)

10.99 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 = log_method

10.99.1 Detailed Description

De nition at line 477 of le https.py.

10.99.2 Member Function Documentation

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

De nition at line 481 of le https.py.

10.99.2.2 def rpki.https.http_listener.handle_accept (self)

De nition at line 502 of le https.py.

10.99.2.3 def rpki.https.http_listener.handle_error (self)

De nition at line 511 of le https.py.

10.99.3 Member Data Documentation

10.99.3.1 rpki.https.http_listener.cert

De nition at line 485 of le https.py.

10.99.3.2 rpki.https.http_listener.dynamic_ta

De nition at line 488 of le https.py.

10.99.3.3 rpki.https.http_listener.handlers

De nition at line 484 of le https.py.

10.99.3.4 rpki.https.http_listener.key

De nition at line 486 of le https.py.

10.99.3.5 rpki.https.http_listener.log = log_method [static]

De nition at line 479 of le https.py.

10.99.3.6 rpki.https.http_listener.ta

De nition at line 487 of le https.py.

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

- https.py (2902)

10.100 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"

10.100.1 Detailed Description

De nition at line 63 of le https.py.

10.100.2 Member Function Documentation

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

De nition at line 67 of le https.py.

10.100.2.2 def rpki.https.http_message.__str__(self)

De nition at line 115 of le https.py.

10.100.2.3 def rpki.https.http_message.format(self)

De nition at line 103 of le https.py.

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

De nition at line 73 of le https.py.

10.100.2.5 def rpki.https.http_message.parse_from_wire(cls, headers)

De nition at line 92 of le https.py.

10.100.2.6 def rpki.https.http_message.parse_version(self, version)

De nition at line 118 of le https.py.

10.100.2.7 def rpki.https.http_message.persistent(self)

De nition at line 123 of le https.py.

10.100.3 Member Data Documentation

10.100.3.1 rpki.https.http_message.body

De nition at line 69 of le https.py.

10.100.3.2 rpki.https.http_message.headers

De nition at line 70 of le https.py.

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

De nition at line 65 of le https.py.

10.100.3.4 rpki.https.http_message.version

De nition at line 68 of le https.py.

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

- https.py (2902)

10.101 rpki.https.http_queue Class Reference

Inheritsobject

Public Member Functions

- def __init__
- def detach
- def request
- def restart
- def return_result
- def send_request

Public Attributes

- cert
- client
- hostport
- key
- queue
- ta

Static Public Attributes

- log = log_method

10.101.1 Detailed Description

De nition at line 634 of le https.py.

10.101.2 Member Function Documentation

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

De nition at line 638 of le https.py.

10.101.2.2 def rpki.https.http_queue.detach (self, client)

De nition at line 673 of le https.py.

10.101.2.3 def rpki.https.http_queue.request (self, requests)

De nition at line 648 of le https.py.

10.101.2.4 def rpki.https.http_queue.restart (self)

De nition at line 652 of le https.py.

10.101.2.5 def rpki.https.http_queue.return_result (self, result)

De nition at line 678 of le https.py.

10.101.2.6 def rpki.https.http_queue.send_requests (self)

De nition at line 669 of le https.py.

10.101.3 Member Data Documentation

10.101.3.1 rpki.https.http_queue.cert

De nition at line 644 of le https.py.

10.101.3.2 rpki.https.http_queue.client

De nition at line 642 of le https.py.

10.101.3.3 rpki.https.http_queue.hostport

De nition at line 641 of le https.py.

10.101.3.4 rpki.https.http_queue.key

De nition at line 645 of le https.py.

10.101.3.5 rpki.https.http_queue.log = log_method[static]

De nition at line 636 of le https.py.

10.101.3.6 rpki.https.http_queue.queue

De nition at line 643 of le https.py.

10.101.3.7 rpki.https.http_queue.ta

De nition at line 646 of le https.py.

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

- https.py (2902)

10.102 rpki.https.http_request Class Reference

Inheritsrpki::https::http_message

Public Member Functions

- def __init__
- def format_ rst_line
- def parse_ rst_line

Public Attributes

- callback
- cmd
- errback
- path
- retried

10.102.1 Detailed Description

De nition at line 132 of le https.py.

10.102.2 Member Function Documentation

10.102.2.1 def rpki.https.http_request.__init__ (self, cmd = None, path = None, version = default_http_version, body = None, callback = None, errback = None, headers = {})

De nition at line 134 of le https.py.

10.102.2.2 def rpki.https.http_request.format_ rst_line (self)

De nition at line 148 of le https.py.

10.102.2.3 def rpki.https.http_request.parse_ rst_line (self, cmd, path, version)

De nition at line 143 of le https.py.

10.102.3 Member Data Documentation

10.102.3.1 rpki.https.http_request.callback

De nition at line 139 of le https.py.

10.102.3.2 rpki.https.http_request.cmd

De nition at line 137 of le https.py.

10.102.3.3 rpki.https.http_request.errback

De nition at line 140 of le https.py.

10.102.3.4 rpki.https.http_request.path

De nition at line 138 of le https.py.

10.102.3.5 rpki.https.http_request.retried

De nition at line 141 of le https.py.

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

- https.py (2902)

10.103 rpki.https.http_response Class Reference

Inherits rpki::https::http_message

Public Member Functions

- def __init__
- def format_ rst_line
- def parse_ rst_line

Public Attributes

- code
- reason

10.103.1 Detailed Description

De nition at line 152 of le https.py.

10.103.2 Member Function Documentation

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

De nition at line 154 of le https.py.

10.103.2.2 def rpki.https.http_response.format_ rst_line (self)

De nition at line 164 of le https.py.

10.103.2.3 def rpki.https.http_response.parse_ rst_line (self, version, code, reason)

De nition at line 159 of le https.py.

10.103.3 Member Data Documentation

10.103.3.1 rpki.https.http_response.code

De nition at line 156 of le https.py.

10.103.3.2 rpki.https.http_response.reason

De nition at line 157 of le https.py.

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

- https.py (2902)

10.104 rpki.https.http_server Class Reference

Inherits rpki::https::http_stream.

Public Member Functions

- def __init__
- def nd_handler
- def handle_message
- def handle_no_content_length
- def send_error
- def send_message
- def send_reply
- def tls_accept

Public Attributes

- expect_close
- handlers
- retry_read
- retry_write
- tls

Static Public Attributes

- parse_type = http_request
- timeout = default_server_timeout

10.104.1 Detailed Description

De nition at line 381 of le https.py.

10.104.2 Member Function Documentation

10.104.2.1 def rpki.https.http_server.__init__ (self, sock, handlers, cert = None, key = None, ta = () , dynamic_ta = None)

De nition at line 387 of le https.py.

10.104.2.2 def rpki.https.http_server. nd_handler (self, path)

Helper method to search self.handlers.

De nition at line 423 of le https.py.

10.104.2.3 def rpki.https.http_server.handle_messages (self)

De nition at line 432 of le https.py.

10.104.2.4 def rpki.https.http_server.handle_no_content_length(self)

De nition at line 420 of le https.py.

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

De nition at line 455 of le https.py.

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

De nition at line 461 of le https.py.

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

De nition at line 458 of le https.py.

10.104.2.8 def rpki.https.http_server.tls_accept(self)

De nition at line 409 of le https.py.

10.104.3 Member Data Documentation

10.104.3.1 rpki.https.http_server.expect_close

De nition at line 391 of le https.py.

10.104.3.2 rpki.https.http_server.handlers

De nition at line 389 of le https.py.

10.104.3.3 rpki.https.http_server.parse_type = http_request[static]

De nition at line 383 of le https.py.

10.104.3.4 rpki.https.http_server.retry_read

Reimplemented from rpki.https.http_stream

De nition at line 413 of le https.py.

10.104.3.5 rpki.https.http_server.retry_write

Reimplemented from rpki.https.http_stream

De nition at line 415 of le https.py.

10.104.3.6 rpki.https.http_server.timeout = default_server_timeout [static]

De nition at line 385 of le https.py.

10.104.3.7 rpki.https.http_server.tls

Reimplemented from rpki.https.http_stream

De nition at line 395 of le https.py.

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

- https.py (2902)

10.105 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 initiate_send
- def log_cert
- def readable
- def recv
- def restart
- def send
- def update_timeout
- def writeable

Public Attributes

- buffer
- chunk_handler
- msg
- timer

Static Public Attributes

- log = log_method
- retry_read = None
- retry_write = None
- tls = None

10.105.1 Detailed Description

De nition at line 174 of le https.py.

10.105.2 Member Function Documentation

10.105.2.1 def rpki.https.http_stream.__init__ (self, sock= None)

De nition at line 181 of le https.py.

10.105.2.2 def rpki.https.http_stream.chunk_body (self)

De nition at line 241 of le https.py.

10.105.2.3 def rpki.https.http_stream.chunk_discard_crlf (self)

De nition at line 248 of le https.py.

10.105.2.4 def rpki.https.http_stream.chunk_discard_trailer (self)

De nition at line 254 of le https.py.

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

De nition at line 231 of le https.py.

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

De nition at line 356 of le https.py.

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

Buffer the data

De nition at line 202 of le https.py.

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

De nition at line 214 of le https.py.

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

De nition at line 209 of le https.py.

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

De nition at line 261 of le https.py.

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

Reimplemented in rpki.https.http_client.

De nition at line 280 of le https.py.

10.105.2.12 def rpki.https.http_stream.handle_error (self)

Reimplemented in rpki.https.http_client.

De nition at line 265 of le https.py.

10.105.2.13 def rpki.https.http_stream.handle_read (self)

De nition at line 301 of le https.py.

10.105.2.14 def rpki.https.http_stream.handle_timeout (self)

Reimplemented in rpki.https.http_client.

De nition at line 276 of le https.py.

10.105.2.15 def rpki.https.http_stream.handle_write (self)

De nition at line 322 of le https.py.

10.105.2.16 def rpki.https.http_stream.initiate_send (self)

De nition at line 341 of le https.py.

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

De nition at line 377 of le https.py.

10.105.2.18 def rpki.https.http_stream.readable (self)

De nition at line 295 of le https.py.

10.105.2.19 def rpki.https.http_stream.recv (self, buffer_size)

De nition at line 290 of le https.py.

10.105.2.20 def rpki.https.http_stream.restart (self)

De nition at line 187 of le https.py.

10.105.2.21 def rpki.https.http_stream.send (self, data)

De nition at line 285 of le https.py.

10.105.2.22 def rpki.https.http_stream.update_timeout (self)

De nition at line 196 of le https.py.

10.105.2.23 def rpki.https.http_stream.writeable (self)

De nition at line 298 of le https.py.

10.105.3 Member Data Documentation

10.105.3.1 rpki.https.http_stream.buffer

De nition at line 183 of le https.py.

10.105.3.2 rpki.https.http_stream.chunk_handler

De nition at line 189 of le https.py.

10.105.3.3 rpki.https.http_stream.log = log_method [static]

De nition at line 176 of le https.py.

10.105.3.4 rpki.https.http_stream.msg

De nition at line 221 of le https.py.

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

Reimplemented in rpki.https.http_server, and rpki.https.http_client.

De nition at line 178 of le https.py.

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

Reimplemented in rpki.https.http_server and rpki.https.http_client

De nition at line 179 of le https.py.

10.105.3.7 rpki.https.http_stream.timer

De nition at line 184 of le https.py.

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

Reimplemented in rpki.https.http_server and rpki.https.http_client

De nition at line 177 of le https.py.

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

- https.py (2902)

10.106 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

10.106.1 Detailed Description

IPv4 address.

Derived from long, but supports IPv4 print syntax.

De nition at line 47 of le ipaddrs.py.

10.106.2 Member Function Documentation

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

Construct a v4addr object.

De nition at line 56 of le ipaddrs.py.

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

Convert a v4addr object to string format.

De nition at line 74 of le ipaddrs.py.

10.106.2.3 def rpki.ipaddrs.v4addr.from_bytes(cls, x)

Convert from a raw byte string to a v4addr object.

De nition at line 70 of le ipaddrs.py.

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

Convert a v4addr object to a raw byte string.

De nition at line 65 of le ipaddrs.py.

10.106.3 Member Data Documentation

10.106.3.1 int rpki.ipaddrs.v4addr.bits = 32 [static]

De nition at line 54 of le ipaddrs.py.

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

- ipaddrs.py (2424)

10.107 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

10.107.1 Detailed Description

IPv6 address.

Derived from long, but supports IPv6 print syntax.

De nition at line 78 of le ipaddrs.py.

10.107.2 Member Function Documentation

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

Construct a v6addr object.

De nition at line 87 of le ipaddrs.py.

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

Convert a v6addr object to string format.

De nition at line 104 of le ipaddrs.py.

10.107.2.3 def rpki.ipaddrs.v6addr.from_bytes (cls, x)

Convert from a raw byte string to a v6addr object.

De nition at line 99 of le ipaddrs.py.

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

Convert a v6addr object to a raw byte string.

De nition at line 94 of le ipaddrs.py.

10.107.3 Member Data Documentation

10.107.3.1 int rpki.ipaddrs.v6addr.bits = 128 [static]

De nition at line 85 of le ipaddrs.py.

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

- ipaddrs.py (2424)

10.108 rpki.left_right.bsc_elt Class Reference

Inherits rpki::left_right::data_elt

Inherited by irbe_cli.bsc_elt

Public Member Functions

- def children
- def parents
- def repositories
- def serve_pre_save_hook

Static Public Attributes

- tuple attributes = ("action", "tag", "self_handle", "bsc_handle", "key_type", "hash_alg", "key_length")

  XML attributes for this element.

- tuple booleans = ("generate_keypair",)

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

- string element_name = "bsc"
- tuple elements = ("signing_cert", "signing_cert_crl", "pkcs10_request")

  XML elements contained by this element.

- tuple handles = (("self", self_elt),)
- pkcs10_request = None
- private_key_id = None
- signing_cert = None
- signing_cert_crl = None
- tuple sql_template

10.108.1 Detailed Description

<bsc/> (Business Signing Context) element.

Definition at line 526 of file left_right.py.

10.108.2 Member Function Documentation

10.108.2.1 def rpki.left_right.bsc_elt.children (self)

Fetch all child objects that link to this BSC object.

Definition at line 557 of file left_right.py.

10.108.2.2 def rpki.left_right.bsc_elt.parents (self)

Fetch all parent objects that link to this BSC object.

Definition at line 553 of file left_right.py.

10.108.2.3 def rpki.left_right.bsc_elt.repositories (self)

Fetch all repository objects that link to this BSC object.

Definition at line 549 of file left_right.py.

10.108.2.4 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 561 of file left_right.py.

10.108.3 Member Data Documentation

10.108.3.1 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 532 of file left_right.py.

10.108.3.2 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 534 of file left_right.py.

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

De nition at line 531 of le left_right.py.

10.108.3.4 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.

De nition at line 533 of le left_right.py.

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

Reimplemented from rpki.left_right.data_elt.

De nition at line 542 of le left_right.py.

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

De nition at line 545 of le left_right.py.

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

De nition at line 544 of le left_right.py.

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

Reimplemented in irbe_cli.bsc_elt.

De nition at line 546 of le left_right.py.

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

Reimplemented in irbe_cli.bsc_elt.

De nition at line 547 of le left_right.py.

10.108.3.10 tuple rpki.left_right.bsc_elt.sql_template [static]

Initial value:

```
rpki.sql.template("bsc",  "bsc_id",  "bsc_handle",
                                                "self_id",  "hash_alg",
                                                ("private_key_id",  rpki.x509.RSA),
                                                ("pkcs10_request",  rpki.x509.PKCS10),
                                                ("signing_cert",  rpki.x509.X509),
                                                ("signing_cert_crl",  rpki.x509.CRL))
```

De nition at line 536 of le left_right.py.

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

- left_right.py (2931)

10.109 rpki.left_right.child_elt Class Reference

Inherits rpki::left_right::data_elt

Inherited by irbe_cli.child_elt

Public Member Functions

- def ca_from_class_name
- def child_certs
- def endElement
- def parents
- def serve_destroy_hook
- def serve_post_save_hook
- def serve_up_down

Static Public Attributes

- tuple attributes = ("action", "tag", "self_handle", "child_handle", "bsc_-handle")

  XML attributes for this element.

- tuple booleans = ("reissue",)

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

- bpki_cert = None
- bpki_glue = None
- clear_https_ta_cache = False
- string element_name = "child"
- tuple elements = ("bpki_cert", "bpki_glue")

  XML elements contained by this element.

- tuple handles = (("self", self_elt), ("bsc", bsc_elt))
- tuple sql_template

10.109.1 Detailed Description

<child/> element.

Definition at line 802 of file left_right.py.

10.109.2 Member Function Documentation

10.109.2.1 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 831 of file left_right.py.

10.109.2.2 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 823 of file left_right.py.

10.109.2.3 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 863 of file left_right.py.

10.109.2.4 def rpki.left_right.child_elt.parents (self)

Fetch all parent objects that link to self object to which this child object links.

De nition at line 827 of le left_right.py.

10.109.2.5 def rpki.left_right.child_elt.serve_destroy_hook (self, cb, eb)

Extra server actions when destroying a child_elt.

Reimplemented from rpki.xml_utils.data_elt.

De nition at line 855 of le left_right.py.

10.109.2.6 def rpki.left_right.child_elt.serve_post_save_hook (self, q_pdu, r_pdu, cb, eb)

Extra server actions for child_elt.

Reimplemented from rpki.xml_utils.data_elt.

De nition at line 845 of le left_right.py.

10.109.2.7 def rpki.left_right.child_elt.serve_up_down (self, query, callback)

Outer layer of server handling for one up-down PDU from this child.

De nition at line 873 of le left_right.py.

10.109.3 Member Data Documentation

10.109.3.1 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.

De nition at line 808 of le left_right.py.

10.109.3.2 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.

De nition at line 810 of le left_right.py.

10.109.3.3 rpki.left_right.child_elt.bpki_cert = None [static]

De nition at line 819 of le left_right.py.

10.109.3.4 rpki.left_right.child_elt.bpki_glue = None [static]

De nition at line 820 of le left_right.py.

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

De nition at line 821 of le left_right.py.

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

De nition at line 807 of le left_right.py.

10.109.3.7 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.

De nition at line 809 of le left_right.py.

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

Reimplemented from rpki.left_right.data_elt

De nition at line 817 of le left_right.py.

10.109.3.9 tuple rpki.left_right.child_elt.sql_template [static]

Initial value:

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

De nition at line 812 of le left_right.py.

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

- left_right.py (2931)

10.110 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

10.110.1 Detailed Description

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

De nition at line 1076 of le left_right.py.

10.110.2 Member Data Documentation

10.110.2.1 string rpki.left_right.cms_msg.encoding = "us-ascii" [static]

De nition at line 1081 of le left_right.py.

10.110.2.2 rpki.left_right.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented in rpki.irbe_cli.left_right_cms_msg.

De nition at line 1083 of le left_right.py.

10.110.2.3 rpki.left_right.cms_msg.schema = rpki.relaxng.left_right [static]

De nition at line 1082 of le left_right.py.

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

- left_right.py (2931)

10.111 rpki.left_right.data_elt Class Reference

Inherits rpki::xml_utils::data_elt, rpki::sql::sql_persistent, and rpki::left_right::left_right_namespace.

Inherited by rpki.left_right.bsc_elt, rpki.left_right.child_elt, rpki.left_right.parent_elt, rpki.left_right.repository_elt, and rpki.left_right.self_elt.

Public Member Functions

- def bsc
- def make_reply_clone_hook
- def self
- def serve_fetch_all
- def serve_fetch_handle
- def serve_fetch_one_maybe
- def serve_pre_save_hook

Static Public Attributes

- tuple handles = ()
- self_handle = None
- self_id = None

10.111.1 Detailed Description

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

De nition at line 50 of le left_right.py.

10.111.2 Member Function Documentation

10.111.2.1 def rpki.left_right.data_elt.bsc (self)

Return BSC object to which this object links.

De nition at line 64 of le left_right.py.

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

Set handles when cloning, including _id -> _handle translation.

Reimplemented from rpki.xml_utils.data_elt.

De nition at line 68 of le left_right.py.

10.111.2.3 def rpki.left_right.data_elt.self (self)

Fetch self object to which this object links.

De nition at line 60 of le left_right.py.

10.111.2.4 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.

De nition at line 99 of le left_right.py.

10.111.2.5 def rpki.left_right.data_elt.serve_fetch_handles(cls, gctx, self_id, handle)

Find an object based on its handle.

Reimplemented in rpki.left_right.self_elt.

De nition at line 84 of le left_right.py.

10.111.2.6 def rpki.left_right.data_elt.serve_fetch_one_maybe(self)

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

Reimplemented in rpki.left_right.self_elt.

De nition at line 90 of le left_right.py.

10.111.2.7 def rpki.left_right.data_elt.serve_pre_save_hook(self, q_pdu, r_pdu, cb, eb)

Hook to do _handle => _id translation before saving.

self is always the object to be saved to SQL. For create operations, self and q_pdu are be the same object; for set operations, self is the pre-existing object from SQL and q_pdu is the set request received from the the IRBE.

Reimplemented from rpki.xml_utils.data_elt.

Reimplemented in rpki.left_right.bsc_elt.

De nition at line 106 of le left_right.py.

10.111.3 Member Data Documentation

10.111.3.1 tuple rpki.left_right.data_elt.handles = () [static]

Reimplemented in rpki.left_right.self_elt, rpki.left_right.bsc_elt, rpki.left_right.repository_elt, rpki.left_right.parent_elt, and rpki.left_right.child_elt.

De nition at line 55 of le left_right.py.

10.111.3.2 rpki.left_right.data_elt.self_handle = None [static]

De nition at line 58 of le left_right.py.

10.111.3.3 rpki.left_right.data_elt.self_id = None [static]

De nition at line 57 of le left_right.py.

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

- left_right.py (2931)

10.112 rpki.left_right.left_right_namespace Class Reference

Inherits object.

Inherited by rpki.left_right.data_elt, rpki.left_right.list_published_objects_elt, rpki.left_right.list_resources_elt, rpki.left_right.list_roa_requests_elt, rpki.left_right.msg, and rpki.left_right.report_error_elt.

Static Public Attributes

- dictionary nsmap = { None : xmlns }
- string xmlns = "http://www.hactrn.net/uris/rpki/left-right-spec/"

10.112.1 Detailed Description

XML namespace parameters for left-right protocol.

De nition at line 42 of le left_right.py.

10.112.2 Member Data Documentation

10.112.2.1 dictionary rpki.left_right.left_right_namespace.nsmap = { None : xmlns } [static]

Definition at line 48 of file left_right.py.

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

Definition at line 47 of file left_right.py.

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

- left_right.py (2931)

10.113 rpki.left_right.list_published_objects_elt Class Reference

Inherits rpki::xml_utils::text_elt, and rpki::left_right::left_right_namespace.

Inherited by irbe_cli.list_published_objects_elt.

Public Member Functions

- def make_reply
- def serve_dispatch

Static Public Attributes

- tuple attributes = ("self_handle", "tag", "uri")

  XML attributes for this element.

- string element_name = "list_published_objects"
- obj = None
- string text_attribute = "obj"

  Name of the class attribute that holds the text value.

10.113.1 Detailed Description

<list_published_objects/> element.

De nition at line 965 of le left_right.py.

10.113.2 Member Function Documentation

10.113.2.1 def rpki.left_right.list_published_objects_elt.make_reply(self, uri, obj)

Generate one reply PDU.

De nition at line 992 of le left_right.py.

10.113.2.2 def rpki.left_right.list_published_objects_elt.serve_dispatch(self, r_msg, cb, eb)

Handle a <list_published_objects/> query. The method name is a misnomer here, there's no action attribute and no dispatch, we just dump every published object for the specified <self/> and return.

De nition at line 976 of le left_right.py.

10.113.3 Member Data Documentation

10.113.3.1 tuple rpki.left_right.list_published_objects_elt.attributes = ("self_handle", "tag", "uri") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

De nition at line 971 of le left_right.py.

10.113.3.2 string rpki.left_right.list_published_objects_elt.element_name = "list_published_objects" [static]

De nition at line 970 of le left_right.py.

10.113.3.3 rpki.left_right.list_published_objects_elt.obj = None [static]

De nition at line 974 of le left_right.py.

10.113.3.4 string rpki.left_right.list_published_objects_elt.text_attribute = "obj" [static]

Name of the class attribute that holds the text value.

Reimplemented from rpki.xml_utils.text_elt.

De nition at line 972 of le left_right.py.

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

- left_right.py (2931)

10.114 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

10.114.1 Detailed Description

<list_resources/> element.

De nition at line 910 of le left_right.py.

10.114.2 Member Function Documentation

10.114.2.1 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.

De nition at line 919 of le left_right.py.

10.114.2.2 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.

De nition at line 935 of le left_right.py.

10.114.3 Member Data Documentation

10.114.3.1 rpki.left_right.list_resources_elt.asn

De nition at line 929 of le left_right.py.

10.114.3.2 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.

De nition at line 916 of le left_right.py.

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

De nition at line 915 of le left_right.py.

10.114.3.4 rpki.left_right.list_resources_elt.ipv4

De nition at line 931 of le left_right.py.

10.114.3.5 rpki.left_right.list_resources_elt.ipv6

De nition at line 933 of le left_right.py.

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

De nition at line 917 of le left_right.py.

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

- left_right.py (2931)

10.115 rpki.left_right.list_roa_requests_elt Class Reference

Inherits rpki::xml_utils::base_elt, and rpki::left_right::left_right_namespace.

Public Member Functions

- def startElement

Public Attributes

- ipv4

- ipv6

Static Public Attributes

- tuple attributes = ("self_handle", "tag", "asn", "ipv4", "ipv6")
  XML attributes for this element.
- string element_name = "list_roa_requests"

10.115.1 Detailed Description

<list_roa_requests/> element.

De nition at line 945 of le left_right.py.

10.115.2 Member Function Documentation

10.115.2.1 def rpki.left_right.list_roa_requests_elt.startElement (self, stack, name, attrs)

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

Reimplemented from rpki.xml_utils.base_elt.

De nition at line 953 of le left_right.py.

10.115.3 Member Data Documentation

10.115.3.1 tuple rpki.left_right.list_roa_requests_elt.attributes = ("self_handle", "tag", "asn", "ipv4", "ipv6") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

De nition at line 951 of le left_right.py.

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

De nition at line 950 of le left_right.py.

10.115.3.3 rpki.left_right.list_roa_requests_elt.ipv4

De nition at line 961 of le left_right.py.

10.115.3.4 rpki.left_right.list_roa_requests_elt.ipv6

De nition at line 963 of le left_right.py.

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

- left_right.py (2931)

10.116 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.

10.116.1 Detailed Description

Left-right PDU.

De nition at line 1023 of le left_right.py.

10.116.2 Member Function Documentation

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

Serve one msg PDU.

De nition at line 1039 of le left_right.py.

10.116.3 Member Data Documentation

10.116.3.1 rpki::left_right.msg::pdus [static]

Initial value:

```
dict((x.element_name, x)
                  for x in (self_elt, child_elt, parent_elt, bsc_elt, repository_elt,
                            list_resources_elt, list_roa_requests_elt, list_published
        _objects_elt,
                            report_error_elt))
```

Dispatch table of PDUs for this protocol.

Reimplemented in rpki.irbe_cli.left_right_msg

De nition at line 1034 of le left_right.py.

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

Protocol version.

Reimplemented from rpki.xml_utils.msg

De nition at line 1030 of le left_right.py.

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

- left_right.py (2931)

10.117 rpki.left_right.parent_elt Class Reference

Inherits rpki::left_right::data_elt

Inherited by irbe_cli.parent_elt

Public Member Functions

- def cas
- def query_up_down
- def repository
- def serve_post_save_hook
- def serve_rekey
- def serve_revoke
- def serve_revoke_forgotten

Static Public Attributes

- tuple attributes

  XML attributes for this element.

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

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

- bpki_cms_cert = None
- bpki_cms_glue = None
- bpki_https_cert = None
- bpki_https_glue = None
- string element_name = "parent"
- tuple elements = ("bpki_cms_cert", "bpki_cms_glue", "bpki_https_cert", "bpki_https_glue")

  XML elements contained by this element.

- tuple handles = (("self", self_elt), ("bsc", bsc_elt), ("repository", repository_elt))
- tuple sql_template

10.117.1 Detailed Description

<parent/> element.

De nition at line 653 of le left_right.py.

10.117.2 Member Function Documentation

10.117.2.1 def rpki.left_right.parent_elt.cas (self)

Fetch all CA objects that link to this parent object.

Definition at line 680 of file left_right.py.

10.117.2.2 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 756 of file left_right.py.

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

Fetch repository object to which this parent object links.

Definition at line 676 of file left_right.py.

10.117.2.4 def rpki.left_right.parent_elt.serve_post_save_hooks (self, q_pdu, r_pdu, cb, eb)

Extra server actions for parent_elt.

Reimplemented from rpki.xml_utils.data_elt

Definition at line 684 of file left_right.py.

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

Handle a left-right rekey action for this parent.

Definition at line 700 of file left_right.py.

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

Handle a left-right revoke action for this parent.

Definition at line 708 of file left_right.py.

10.117.2.7 def rpki.left_right.parent_elt.serve_revoke_forgotten(self, cb, eb)

Handle a left-right revoke_forgotten action for this parent.

This is a bit fiddly: we have to compare the result of an up-down list query with what we have locally and identify the SKIs of any certificates that have gone missing. This should never happen in ordinary operation, but can arise if we have somehow lost a private key, in which case there is nothing more we can do with the issued cert, so we have to clear it. As this really is not supposed to happen, we don't clear it automatically, instead we require an explicit trigger.

Definition at line 716 of file left_right.py.

10.117.3 Member Data Documentation

10.117.3.1 tuple rpki.left_right.parent_elt.attributes [static]

Initial value:

```
("action", "tag", "self_handle", "parent_handle", "bsc_handle", "repository_handl
        e",
                  "peer_contact_uri", "sia_base", "sender_name", "recipient_name")
```

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 659 of file left_right.py.

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

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

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 662 of file left_right.py.

10.117.3.3 rpki.left_right.parent_elt.bpki_cms_cert = None [static]

De nition at line 671 of le left_right.py.

10.117.3.4 rpki.left_right.parent_elt.bpki_cms_glue = None [static]

De nition at line 672 of le left_right.py.

10.117.3.5 rpki.left_right.parent_elt.bpki_https_cert = None [static]

De nition at line 673 of le left_right.py.

10.117.3.6 rpki.left_right.parent_elt.bpki_https_glue = None [static]

De nition at line 674 of le left_right.py.

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

De nition at line 658 of le left_right.py.

10.117.3.8 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.

De nition at line 661 of le left_right.py.

10.117.3.9 tuple rpki.left_right.parent_elt.handles = (("self", self_elt), ("bsc", bsc_elt), ("repository", repository_elt)) [static]

Reimplemented from rpki.left_right.data_elt

De nition at line 669 of le left_right.py.

10.117.3.10 tuple rpki.left_right.parent_elt.sql_template [static]

Initial value:

```
rpki.sql.template("parent", "parent_id", "parent_handle",
                                                "self_id", "bsc_id", "repository_id",
                                                ("bpki_cms_cert", rpki.x509.X509), ("bpki_cms_
        glue", rpki.x509.X509),
                                                ("bpki_https_cert", rpki.x509.X509), ("bpki_ht
        tps_glue", rpki.x509.X509),
                                                "peer_contact_uri", "sia_base", "sender_name",
         "recipient_name")
```

De nition at line 664 of le left_right.py.

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

- left_right.py (2931)

10.118 rpki.left_right.report_error_elt Class Reference

Inherits rpki::xml_utils::text_elt, and rpki::left_right::left_right_namespace

Inherited by irbe_cli.report_error_elt

Public Member Functions

- def from_exception

Public Attributes

- error_code
- self_handle
- tag

Static Public Attributes

- tuple attributes = ("tag", "self_handle", "error_code")
  XML attributes for this element.
- string element_name = "report_error"
- error_text = None
- string text_attribute = "error_text"
  Name of the class attribute that holds the text value.

10.118.1 Detailed Description

<report_error/> element.

De nition at line 1000 of le left_right.py.

10.118.2 Member Function Documentation

10.118.2.1 def rpki.left_right.report_error_elt.from_exception (cls, e, self_handle = None, tag = None)

Generate a <report_error/> element from an exception.

De nition at line 1012 of le left_right.py.

10.118.3 Member Data Documentation

10.118.3.1 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.

De nition at line 1006 of le left_right.py.

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

De nition at line 1005 of le left_right.py.

10.118.3.3 rpki.left_right.report_error_elt.error_code

De nition at line 1019 of le left_right.py.

10.118.3.4 rpki.left_right.report_error_elt.error_text = None [static]

De nition at line 1009 of le left_right.py.

10.118.3.5 rpki.left_right.report_error_elt.self_handle

De nition at line 1017 of le left_right.py.

10.118.3.6 rpki.left_right.report_error_elt.tag

De nition at line 1018 of le left_right.py.

10.118.3.7 string rpki.left_right.report_error_elt.text_attribute = "error_text" [static]

Name of the class attribute that holds the text value.

Reimplemented from rpki.xml_utils.text_elt.

De nition at line 1007 of le left_right.py.

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

- left_right.py (2931)

10.119 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 default_pubd_handler
- def parents

Static Public Attributes

- tuple attributes = ("action", "tag", "self_handle", "repository_handle", "bsc_handle", "peer_contact_uri")

  XML attributes for this element.

- bpki_cert = None
- bpki_glue = None
- string element_name = "repository"
- tuple elements = ("bpki_cert", "bpki_glue")

  XML elements contained by this element.

- tuple handles = (("self", self_elt), ("bsc", bsc_elt))
- tuple sql_template

10.119.1 Detailed Description

<repository/> element.

De nition at line 573 of le left_right.py.

10.119.2 Member Function Documentation

10.119.2.1 def rpki.left_right.repository_elt.call_pubd (self, callback, errback, q_msg, handlers = {})

Send a message to publication daemon and return the response.

As a convenience, attempting to send an empty message returns immediate success without sending anything.

Handlers is a dict of handler functions to process the response PDUs. If the tag value in the response PDU appears in the dict, the associated handler is called to process the PDU. If no tag matches, default_pubd_handler() is called. A handler value of False suppresses calling of the default handler.

De nition at line 601 of le left_right.py.

10.119.2.2 def rpki.left_right.repository_elt.default_pubd_handler (pdu)

Default handler for publication response PDUs.

De nition at line 595 of le left_right.py.

10.119.2.3 def rpki.left_right.repository_elt.parents (self)

Fetch all parent objects that link to this repository object.

De nition at line 590 of le left_right.py.

10.119.3 Member Data Documentation

10.119.3.1 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.

De nition at line 579 of le left_right.py.

10.119.3.2 rpki.left_right.repository_elt.bpki_cert = None [static]

De nition at line 587 of le left_right.py.

10.119.3.3 rpki.left_right.repository_elt.bpki_glue = None [static]

De nition at line 588 of le left_right.py.

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

De nition at line 578 of le left_right.py.

10.119.3.5 tuple rpki.left_right.repository_elt.elements = ("bpki_cert", "bpki_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

De nition at line 580 of le left_right.py.

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

Reimplemented from rpki.left_right.data_elt.

De nition at line 585 of le left_right.py.

10.119.3.7 tuple rpki.left_right.repository_elt.sql_template [static]

Initial value:

```
rpki.sql.template("repository", "repository_id", "repository_handle",
                                                 "self_id", "bsc_id", "peer_contact_uri",
                                                 ("bpki_cert", rpki.x509.X509), ("bpki_glue", r
    pki.x509.X509))
```

De nition at line 582 of le left_right.py.

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

- left_right.py (2931)

10.120 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"

10.120.1 Detailed Description

SAX handler for Left-Right protocol.

De nition at line 1067 of le left_right.py.

10.120.2 Member Data Documentation

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

De nition at line 1073 of le left_right.py.

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

Reimplemented in rpki.irbe_cli.left_right_sax_handler.

De nition at line 1072 of le left_right.py.

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

De nition at line 1074 of le left_right.py.

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

- left_right.py (2931)

10.121 rpki.left_right.self_elt Class Reference

Inherits rpki::left_right::data_elt.

Inherited by rpki.irbe_cli.self_elt.

Public Member Functions

- def bscs

- def children
- def client_poll
- def cron
- def parents
- def regenerate_crls_and_manifests
- def repositories
- def roas
- def serve_fetch_all
- def serve_fetch_handle
- def serve_fetch_one_maybe
- def serve_post_save_hook
- def serve_publish_world_now
- def serve_rekey
- def serve_revoke
- def serve_revoke_forgotten
- def serve_run_now
- def update_children
- def update_roas

Static Public Attributes

- tuple attributes = ("action", "tag", "self_handle", "crl_interval", "regen_-margin")

  XML attributes for this element.

- tuple booleans= ("rekey", "reissue", "revoke", "run_now", "publish_world_-now", "revoke_forgotten")

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

- bpki_cert= None
- bpki_glue= None
- crl_interval= None
- string element_name= "self"
- tuple elements= ("bpki_cert", "bpki_glue")

  XML elements contained by this element.

- tuple handles= ()
- regen_margin= None
- tuple sql_template
- use_hsm= False

10.121.1 Detailed Description

<self/> element.

De nition at line 124 of le left_right.py.

10.121.2 Member Function Documentation

10.121.2.1 def rpki.left_right.self_elt.bscs (self)

Fetch all BSC objects that link to this self object.

De nition at line 145 of le left_right.py.

10.121.2.2 def rpki.left_right.self_elt.children (self)

Fetch all child objects that link to this self object.

De nition at line 157 of le left_right.py.

10.121.2.3 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.

De nition at line 302 of le left_right.py.

10.121.2.4 def rpki.left_right.self_elt.cron (self, cb)

Periodic tasks.

De nition at line 274 of le left_right.py.

10.121.2.5 def rpki.left_right.self_elt.parents (self)

Fetch all parent objects that link to this self object.

De nition at line 153 of le left_right.py.

10.121.2.6 def rpki.left_right.self_elt.regenerate_crls_and_manifests (self, cb)

Generate new CRLs and manifests as necessary for all of this self's CAs. Extracting nextUpdate from a manifest is hard at the moment due to implementation silliness, so for now we generate a new manifest whenever we generate a new CRL

This method also cleans up tombstones left behind by revoked ca_detail objects, since we're walking through the relevant portions of the database anyway.

De nition at line 428 of le left_right.py.

10.121.2.7 def rpki.left_right.self_elt.repositories (self)

Fetch all repository objects that link to this self object.

De nition at line 149 of le left_right.py.

10.121.2.8 def rpki.left_right.self_elt.roas (self)

Fetch all ROA objects that link to this self object.

De nition at line 161 of le left_right.py.

10.121.2.9 def rpki.left_right.self_elt.serve_fetch_all (self)

Find the self objects upon which a list action should operate. This is different from the list action for all other objects, where list only works within a given self_id context.

Reimplemented from rpki.left_right.data_elt

De nition at line 266 of le left_right.py.

10.121.2.10 def rpki.left_right.self_elt.serve_fetch_handles(cls, gctx, self_id, self_handle)

Find a self object based on its self_handle.

Reimplemented from rpki.left_right.data_elt

De nition at line 260 of le left_right.py.

10.121.2.11 def rpki.left_right.self_elt.serve_fetch_one_maybe(self)

Find the self object upon which a get, set, or destroy action should operate, or which would conflict with a create method.

Reimplemented from rpki.left_right.data_elt

De nition at line 252 of le left_right.py.

10.121.2.12 def rpki.left_right.self_elt.serve_post_save_hook(self, q_pdu, r_pdu, cb, eb)

Extra server actions for self_elt.

Reimplemented from rpki.xml_utils.data_elt

De nition at line 165 of le left_right.py.

10.121.2.13 def rpki.left_right.self_elt.serve_publish_world_now(self, cb, eb)

Handle a left-right publish_world_now action for this self.

The publication stuff needs refactoring, right now publication is interleaved with local operations in a way that forces far too many bounces through the task system for any complex update. The whole thing ought to be rewritten to queue up outgoing publication

PDUs and only send them when we're all done or when we need to force publication at a particular point in a multi-phase operation.

Once that reorganization has been done, this method should be rewritten to reuse the low-level publish() methods that each object will have...but we're not there yet. So, for now, we just do this via brute force. Think of it as a trial version to see whether we've identified everything that needs to be republished for this operation.

Definition at line 213 of file left_right.py.

10.121.2.14 def rpki.left_right.self_elt.serve_rekeys(self, cb, eb)

Handle a left-right rekey action for this self.

Definition at line 186 of file left_right.py.

10.121.2.15 def rpki.left_right.self_elt.serve_revokes(self, cb, eb)

Handle a left-right revoke action for this self.

Definition at line 195 of file left_right.py.

10.121.2.16 def rpki.left_right.self_elt.serve_revoke_forgottens(self, cb, eb)

Handle a left-right revoke_forgotten action for this self.

Definition at line 204 of file left_right.py.

10.121.2.17 def rpki.left_right.self_elt.serve_run_nows(self, cb, eb)

Handle a left-right run_now action for this self.

Definition at line 245 of file left_right.py.

10.121.2.18 def rpki.left_right.self_elt.update_children (self, cb)

Check for updated IRDB data for all of this self's children and issue new certs as necessary. Must handle changes both in resources and in expiration date.

De nition at line 361 of le left_right.py.

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

Generate or update ROAs for this self.

De nition at line 470 of le left_right.py.

10.121.3 Member Data Documentation

10.121.3.1 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.

De nition at line 130 of le left_right.py.

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

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

Reimplemented from rpki.xml_utils.base_elt.

De nition at line 132 of le left_right.py.

10.121.3.3 rpki.left_right.self_elt.bpki_cert = None [static]

De nition at line 142 of le left_right.py.

10.121.3.4 rpki.left_right.self_elt.bpki_glue = None [static]

De nition at line 143 of le left_right.py.

10.121.3.5 rpki.left_right.self_elt.crl_interval = None [static]

De nition at line 140 of le left_right.py.

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

De nition at line 129 of le left_right.py.

10.121.3.7 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.

De nition at line 131 of le left_right.py.

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

Reimplemented from rpki.left_right.data_elt.

De nition at line 137 of le left_right.py.

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

De nition at line 141 of le left_right.py.

10.121.3.10 tuple rpki.left_right.self_elt.sql_template [static]

Initial value:

```
rpki.sql.template("self", "self_id", "self_handle",
                                                "use_hsm", "crl_interval", "regen_margin",
                                                ("bpki_cert", rpki.x509.X509), ("bpki_glue", r
        pki.x509.X509))
```

De nition at line 134 of le left_right.py.

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

De nition at line 139 of le left_right.py.

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

- left_right.py (2931)

10.122 rpki.log.logger Class Reference

Inherits object.

Public Member Functions

- def __call__
- def __init__

Public Attributes

- priority

10.122.1 Detailed Description

Closure for logging.

De nition at line 71 of le log.py.

10.122.2 Member Function Documentation

10.122.2.1 def rpki.log.logger.__call__(self, message)

De nition at line 79 of le log.py.

10.122.2.2 def rpki.log.logger.__init__ (self, priority)

De nition at line 76 of le log.py.

10.122.3 Member Data Documentation

10.122.3.1 rpki.log.logger.priority

De nition at line 77 of le log.py.

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

- log.py (2933)

10.123 rpki.manifest.FileAndHash Class Reference

Inherits Sequence.

Public Member Functions

- def __init__

Public Attributes

- le
- hash

10.123.1 Detailed Description

De nition at line 27 of le manifest.py.

10.123.2 Member Function Documentation

10.123.2.1 def rpki.manifest.FileAndHash.__init__ (self, optional = 0, default = ”)

De nition at line 28 of le manifest.py.

10.123.3 Member Data Documentation

10.123.3.1 rpki.manifest.FileAndHash. le

De nition at line 29 of le manifest.py.

10.123.3.2 rpki.manifest.FileAndHash.hash

De nition at line 30 of le manifest.py.

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

- manifest.py (2424)

10.124 rpki.manifest.FilesAndHashes Class Reference

InheritsSequenceOf

Public Member Functions

- def __init__

10.124.1 Detailed Description

De nition at line 34 of le manifest.py.

10.124.2 Member Function Documentation

10.124.2.1 def rpki.manifest.FilesAndHashes.__init__(self, optional = 0, default = '')

De nition at line 35 of le manifest.py.

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

- manifest.py (2424)

10.125 rpki.manifest.Manifest Class Reference

Inherits Sequence.

Public Member Functions

- def __init__

Public Attributes

- explicitVersion
- leHashAlg
- leList
- manifestNumber
- nextUpdate
- thisUpdate
- version

10.125.1 Detailed Description

De nition at line 38 of le manifest.py.

10.125.2 Member Function Documentation

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

De nition at line 39 of le manifest.py.

10.125.3 Member Data Documentation

10.125.3.1 rpki.manifest.Manifest.explicitVersion

De nition at line 41 of le manifest.py.

10.125.3.2 rpki.manifest.Manifest. leHashAlg

De nition at line 45 of le manifest.py.

10.125.3.3 rpki.manifest.Manifest. leList

De nition at line 46 of le manifest.py.

10.125.3.4 rpki.manifest.Manifest.manifestNumber

De nition at line 42 of le manifest.py.

10.125.3.5 rpki.manifest.Manifest.nextUpdate

De nition at line 44 of le manifest.py.

10.125.3.6 rpki.manifest.Manifest.thisUpdate

De nition at line 43 of le manifest.py.

10.125.3.7 rpki.manifest.Manifest.version

De nition at line 40 of le manifest.py.

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

- manifest.py (2424)

10.126 rpki.publication.certi cate_elt Class Reference

Inherits rpki::publication::publication_object_elt

Inherited by irbe_cli.certi cate_elt

Static Public Attributes

- string element_name = "certi cate"
- payload_type = rpki.x509.X509

10.126.1 Detailed Description

<certificate/> element.

De nition at line 286 of le publication.py.

10.126.2 Member Data Documentation

10.126.2.1 string rpki.publication.certi cate_elt.element_name = "certi cate" [static]

De nition at line 291 of le publication.py.

10.126.2.2 rpki.publication.certi cate_elt.payload_type = rpki.x509.X509 [static]

Reimplemented from rpki.publication.publication_object_elt.

De nition at line 292 of le publication.py.

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

- publication.py (2935)

10.127 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))

10.127.1 Detailed Description

<client/> element.

Definition at line 113 of file publication.py.

10.127.2 Member Function Documentation

10.127.2.1 def rpki.publication.client_elt.check_allowed_uri(self, uri)

Definition at line 160 of file publication.py.

10.127.2.2 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.

10.127.2.3 def rpki.publication.client_elt.serve_fetch_all(self)

Find client objects on which a list method should operate.

De nition at line 156 of le publication.py.

10.127.2.4 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.

De nition at line 149 of le publication.py.

10.127.2.5 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.

De nition at line 140 of le publication.py.

10.127.3 Member Data Documentation

10.127.3.1 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.

De nition at line 119 of le publication.py.

10.127.3.2 rpki.publication.client_elt.base_uri = None [static]

De nition at line 124 of le publication.py.

10.127.3.3 rpki.publication.client_elt.bpki_cert = None [static]

De nition at line 125 of le publication.py.

10.127.3.4 rpki.publication.client_elt.bpki_glue = None [static]

De nition at line 126 of le publication.py.

10.127.3.5 rpki.publication.client_elt.clear_https_ta_cache = False [static]

De nition at line 128 of le publication.py.

10.127.3.6 string rpki.publication.client_elt.element_name = "client" [static]

De nition at line 118 of le publication.py.

10.127.3.7 tuple rpki.publication.client_elt.elements = ("bpki_cert", "bpki_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

De nition at line 120 of le publication.py.

10.127.3.8 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]

De nition at line 122 of le publication.py.

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

- publication.py (2935)

10.128 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

10.128.1 Detailed Description

Class to hold a CMS-signed publication PDU.

De nition at line 414 of le publication.py.

10.128.2 Member Data Documentation

10.128.2.1 string rpki.publication.cms_msg.encoding = "us-ascii" [static]

De nition at line 419 of le publication.py.

10.128.2.2 rpki.publication.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented in irbe_cli.publication_cms_msg.

De nition at line 421 of le publication.py.

10.128.2.3 rpki.publication.cms_msg.schema = rpki.relaxng.publication [static]

De nition at line 420 of le publication.py.

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

- publication.py (2935)

10.129 rpki.publication.con g_elt Class Reference

Inherits rpki::publication::control_elt

Inherited by irbe_cli.con g_elt.

Public Member Functions

- def fetch
- def serve_fetch_one_maybe
- def serve_set
- def startElement

Public Attributes

- con g_id

Static Public Attributes

- tuple attributes = ("action", "tag")

  XML attributes for this element.

- string element_name = "con g"
- tuple elements = ("bpki_crl",)

  XML elements contained by this element.

- tuple sql_template = rpki.sql.template("con g", "con g_id", ("bpki_crl", rpki.x509.CRL))
- int wired_in_con g_id = 1

10.129.1 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.

De nition at line 61 of le publication.py.

10.129.2 Member Function Documentation

10.129.2.1 def rpki.publication.con g_elt.fetch (cls, gctx)

Fetch the config object from SQL. This requires special handling because of the weird way we treat config_id.

De nition at line 89 of le publication.py.

10.129.2.2 def rpki.publication.con g_elt.serve_fetch_one_maybe (self)

Find the config object on which a get or set method should operate.

De nition at line 106 of le publication.py.

10.129.2.3 def rpki.publication.con g_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.

De nition at line 96 of le publication.py.

10.129.2.4 def rpki.publication.con g_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.

De nition at line 80 of le publication.py.

10.129.3 Member Data Documentation

10.129.3.1 tuple rpki.publication.con g_elt.attributes = ("action", "tag") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

De nition at line 72 of le publication.py.

10.129.3.2 rpki.publication.con g_elt.con g_id

De nition at line 86 of le publication.py.

10.129.3.3 string rpki.publication.con g_elt.element_name = "con g" [static]

De nition at line 73 of le publication.py.

10.129.3.4 tuple rpki.publication.con g_elt.elements = ("bpki_crl",) [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

De nition at line 74 of le publication.py.

10.129.3.5 tuple rpki.publication.con g_elt.sql_template = rpki.sql.template("con g", "con g_id", ("bpki_crl", rpki.x509.CRL)) [static]

De nition at line 76 of le publication.py.

10.129.3.6 int rpki.publication.con g_elt.wired_in_con g_id = 1 [static]

De nition at line 78 of le publication.py.

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

- publication.py (2935)

10.130 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.con g_elt.

Public Member Functions

- def serve_dispatch

10.130.1 Detailed Description

Virtual class for control channel objects.

De nition at line 47 of le publication.py.

10.130.2 Member Function Documentation

10.130.2.1 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.

De nition at line 52 of le publication.py.

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

- publication.py (2935)

10.131 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

10.131.1 Detailed Description

<crl/> element.

De nition at line 294 of le publication.py.

10.131.2 Member Data Documentation

10.131.2.1 string rpki.publication.crl_elt.element_name = "crl" [static]

De nition at line 299 of le publication.py.

10.131.2.2 rpki.publication.crl_elt.payload_type = rpki.x509.CRL [static]

Reimplemented from rpki.publication.publication_object_elt

De nition at line 300 of le publication.py.

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

- publication.py (2935)

10.132 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

10.132.1 Detailed Description

<manifest/> element.

De nition at line 302 of le publication.py.

10.132.2 Member Data Documentation

10.132.2.1 string rpki.publication.manifest_elt.element_name = "manifest" [static]

De nition at line 307 of le publication.py.

10.132.2.2 rpki.publication.manifest_elt.payload_type = rpki.x509.SignedManifest [static]

Reimplemented from rpki.publication.publication_object_elt

De nition at line 308 of le publication.py.

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

- publication.py (2935)

10.133 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.

10.133.1 Detailed Description

Publication PDU.

De nition at line 361 of le publication.py.

10.133.2 Member Function Documentation

10.133.2.1 def rpki.publication.msg.serve_top_level(self, gctx, client, cb)

Serve one msg PDU.

De nition at line 375 of le publication.py.

10.133.3 Member Data Documentation

10.133.3.1 rpki::publication.msg::pdus [static]

Initial value:

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

Dispatch table of PDUs for this protocol.

Reimplemented in rpkid_cli.publication_msg.

De nition at line 372 of le publication.py.

10.133.3.2 rpki::publication.msg::version = 1 [static]

Protocol version.

Reimplemented from rpki.xml_utils.msg.

De nition at line 368 of le publication.py.

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

- publication.py (2935)

10.134 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/"

10.134.1 Detailed Description

XML namespace parameters for publication protocol.

De nition at line 39 of le publication.py.

10.134.2 Member Data Documentation

10.134.2.1 dictionary rpki.publication.publication_namespace.nsmap = { None : xmlns } [static]

De nition at line 45 of le publication.py.

10.134.2.2 string rpki.publication.publication_namespace.xmlns = "http://www.hactrn.net/uris/rpki/publication-spec/" [static]

De nition at line 44 of le publication.py.

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

- publication.py (2935)

10.135 rpki.publication.publication_object_elt Class Reference

Inherits rpki::xml_utils::base_elt, and rpki::publication::publication_namespace

Inherited by rpki.publication.certificate_elt, rpki.publication.crl_elt, rpki.publication.manifest_elt, and rpki.publication.roa_elt.

Public Member Functions

- def endElement
- def make_publish
- def make_withdraw
- def raise_if_error
- def serve_dispatch
- def serve_publish
- def serve_withdraw
- def toXML
- def uri_to_filename

Static Public Attributes

- tuple attributes = ("action", "tag", "client_handle", "uri")

  XML attributes for this element.

- payload = None
- payload_type = None

10.135.1 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.

10.135.2 Member Function Documentation

10.135.2.1 def rpki.publication.publication_object_elt.endElement(self, stack, name, text)

Handle a publishable element element.

Reimplemented from rpki.xml_utils.base_elt.

De nition at line 178 of le publication.py.

10.135.2.2 def rpki.publication.publication_object_elt.make_publish(cls, uri, obj, tag = None)

Construct a publication PDU.

De nition at line 265 of le publication.py.

10.135.2.3 def rpki.publication.publication_object_elt.make_withdraw(cls, uri, obj, tag = None)

Construct a withdrawal PDU.

De nition at line 273 of le publication.py.

10.135.2.4 def rpki.publication.publication_object_elt.raise_if_error(self)

No-op, since this is not a <report_error/> PDU.

De nition at line 280 of le publication.py.

10.135.2.5 def rpki.publication.publication_object_elt.serve_dispatch(self, r_msg, cb, eb)

Action dispatch handler.

De nition at line 196 of le publication.py.

10.135.2.6 def rpki.publication.publication_object_elt.serve_publish (self)

Publish an object.

Definition at line 221 of file publication.py.

10.135.2.7 def rpki.publication.publication_object_elt.serve_withdraw (self)

Withdraw an object.

Definition at line 236 of file publication.py.

10.135.2.8 def rpki.publication.publication_object_elt.toXML (self)

Generate XML element for publishable object.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 187 of file publication.py.

10.135.2.9 def rpki.publication.publication_object_elt.uri_to_filename (self)

Convert a URI to a local filename.

Definition at line 250 of file publication.py.

10.135.3 Member Data Documentation

10.135.3.1 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.

10.135.3.2 rpki.publication.publication_object_elt.payload = None [static]

De nition at line 176 of le publication.py.

10.135.3.3 rpki.publication.publication_object_elt.payload_type = None [static]

Reimplemented in rpki.publication.certi cate_elt, rpki.publication.crl_elt, rpki.publication.manifest_elt, and rpki.publication.roa_elt.

De nition at line 175 of le publication.py.

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

- publication.py (2935)

10.136 rpki.publication.report_error_elt Class Reference

Inherits rpki::xml_utils::text_elt, and rpki::publication::publication_namespace.

Inherited by irbe_cli.report_error_elt.

Public Member Functions

- def __str__
- def from_exception
- def raise_if_error

Public Attributes

- error_code
- tag

Static Public Attributes

- tuple attributes = ("tag", "error_code")

  XML attributes for this element.

- string element_name = "report_error"
- error_text = None

- string text_attribute = "error_text"
  Name of the class attribute that holds the text value.

10.136.1 Detailed Description

<report_error/> element.

Definition at line 320 of file publication.py.

10.136.2 Member Function Documentation

10.136.2.1 def rpki.publication.report_error_elt.__str__ (self)

Convert a base_elt object to string format.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 342 of file publication.py.

10.136.2.2 def rpki.publication.report_error_elt.from_exception (cls, e, tag = None)

Generate a <report_error/> element from an exception.

Definition at line 332 of file publication.py.

10.136.2.3 def rpki.publication.report_error_elt.raise_if_error (self)

Raise exception associated with this <report_error/> PDU.

Definition at line 351 of file publication.py.

10.136.3 Member Data Documentation

10.136.3.1 tuple rpki.publication.report_error_elt.attributes = ("tag", "error_code") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

De nition at line 326 of le publication.py.

10.136.3.2 string rpki.publication.report_error_elt.element_name = "report_error" [static]

De nition at line 325 of le publication.py.

10.136.3.3 rpki.publication.report_error_elt.error_code

De nition at line 338 of le publication.py.

10.136.3.4 rpki.publication.report_error_elt.error_text = None [static]

De nition at line 329 of le publication.py.

10.136.3.5 rpki.publication.report_error_elt.tag

De nition at line 337 of le publication.py.

10.136.3.6 string rpki.publication.report_error_elt.text_attribute = "error_text" [static]

Name of the class attribute that holds the text value.

Reimplemented from rpki.xml_utils.text_elt.

De nition at line 327 of le publication.py.

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

- publication.py (2935)

10.137 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

10.137.1 Detailed Description

<roa/> element.

Definition at line 310 of file publication.py.

10.137.2 Member Data Documentation

10.137.2.1 string rpki.publication.roa_elt.element_name = "roa" [static]

Definition at line 315 of file publication.py.

10.137.2.2 rpki.publication.roa_elt.payload_type = rpki.x509.ROA [static]

Reimplemented from rpki.publication.publication_object_elt.

Definition at line 316 of file publication.py.

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

- publication.py (2935)

10.138 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"

10.138.1 Detailed Description

SAX handler for publication protocol.

De nition at line 405 of le publication.py.

10.138.2 Member Data Documentation

10.138.2.1 string rpki.publication.sax_handler.name = "msg" [static]

De nition at line 411 of le publication.py.

10.138.2.2 rpki.publication.sax_handler.pdu = msg [static]

Reimplemented in irbe_cli.publication_sax_handler
De nition at line 410 of le publication.py.

10.138.2.3 string rpki.publication.sax_handler.version = "1" [static]

De nition at line 412 of le publication.py.
The documentation for this class was generated from the following le:

- publication.py (2935)

10.139 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 certi cate notAfter eld.

10.139.1 Detailed Description

Container to simplify passing around the usual triple of ASN, IPv4, and IPv6 resource sets.

De nition at line 547 of le resource_set.py.

10.139.2 Member Function Documentation

10.139.2.1 def rpki.resource_set.resource_bag.__eq__(self, other)

De nition at line 615 of le resource_set.py.

10.139.2.2 def rpki.resource_set.resource_bag.__init__(self, asn = None, v4 = None, v6 = None, valid_until = None)

De nition at line 565 of le resource_set.py.

10.139.2.3 def rpki.resource_set.resource_bag.__ne__(self, other)

De nition at line 621 of le resource_set.py.

10.139.2.4 def rpki.resource_set.resource_bag.__str__(self)

De nition at line 644 of le resource_set.py.

10.139.2.5 def rpki.resource_set.resource_bag.empty(self)

True iff all resource sets in this bag are empty.

De nition at line 611 of le resource_set.py.

10.139.2.6 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.

De nition at line 588 of le resource_set.py.

10.139.2.7 def rpki.resource_set.resource_bag.intersection(self, other)

Compute intersection with another resource_bag. valid_until attribute (if any) inherits from self.

De nition at line 624 of le resource_set.py.

10.139.2.8 def rpki.resource_set.resource_bag.oversized(self, other)

True iff self is oversized with respect to other.

De nition at line 571 of le resource_set.py.

10.139.2.9 def rpki.resource_set.resource_bag.undersized(self, other)

True iff self is undersized with respect to other.

De nition at line 579 of le resource_set.py.

10.139.2.10 def rpki.resource_set.resource_bag.union(self, other)

Compute union with another resource_bag. valid_until attribute (if any) inherits from self.

De nition at line 634 of le resource_set.py.

10.139.3 Member Data Documentation

10.139.3.1 rpki::resource_set.resource_bag::asn

Set of Autonomous System Number resources.

De nition at line 566 of le resource_set.py.

10.139.3.2 rpki::resource_set.resource_bag::v4

Set of IPv4 resources.

De nition at line 567 of le resource_set.py.

10.139.3.3 rpki::resource_set.resource_bag::v6

Set of IPv6 resources.

De nition at line 568 of le resource_set.py.

10.139.3.4 rpki::resource_set.resource_bag::valid_until

Expiration date of resources, for setting certi cate notAfter eld.

De nition at line 569 of le resource_set.py.

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

- resource_set.py (2776)

10.140 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

10.140.1 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.

De nition at line 50 of le resource_set.py.

10.140.2 Member Function Documentation

10.140.2.1 def rpki.resource_set.resource_range.__cmp__(self, other)

Compare two resource_range objects.

Definition at line 67 of file resource_set.py.

10.140.2.2 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.

10.140.3 Member Data Documentation

10.140.3.1 rpki.resource_set.resource_range.max

Definition at line 65 of file resource_set.py.

10.140.3.2 rpki.resource_set.resource_range.min

Reimplemented in rpki.resource_set.resource_range_as.

Definition at line 64 of file resource_set.py.

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

- resource_set.py (2776)

10.141 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).

10.141.1 Detailed Description

Range of Autonomous System Numbers.

Denotes a single ASN by a range whose min and max values are identical.

De nition at line 78 of le resource_set.py.

10.141.2 Member Function Documentation

10.141.2.1 def rpki.resource_set.resource_range_as.__str__(self)

Convert a resource_range_as to string format.

De nition at line 91 of le resource_set.py.

10.141.2.2 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.

De nition at line 100 of le resource_set.py.

10.141.3 Member Data Documentation

10.141.3.1 rpki::resource_set.resource_range_as::datum_type = long [static]

Type of underlying data (min and max).

De nition at line 89 of le resource_set.py.

10.141.3.2 rpki.resource_set.resource_range_as.min

Reimplemented from rpki.resource_set.resource_range.

De nition at line 95 of le resource_set.py.

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

- resource_set.py (2776)

10.142 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_pre x
- def to_rfc3779_tuple

Private Member Functions

- def _pre xlen

10.142.1 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.

De nition at line 109 of le resource_set.py.

10.142.2 Member Function Documentation

10.142.2.1 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.

10.142.2.2 def rpki.resource_set.resource_range_ip._prefix_xlen(self) [private]

Determine whether a resource_range_ip can be expressed as a prefix.

Definition at line 120 of file resource_set.py.

10.142.2.3 def rpki.resource_set.resource_range_ip.make_prefix(cls, prefix, prefixlen)

Construct a resource range corresponding to a prefix.

Definition at line 160 of file resource_set.py.

10.142.2.4 def rpki.resource_set.resource_range_ip.to_rfc3779_tuple(self)

Convert a resource_range_ip to tuple format for RFC 3779 ASN.1 encoding.

Definition at line 147 of file resource_set.py.

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

- resource_set.py (2776)

10.143 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).

10.143.1 Detailed Description

Range of IPv4 addresses.

De nition at line 170 of le resource_set.py.

10.143.2 Member Data Documentation

10.143.2.1 rpki::resource_set.resource_range_ipv4::datum_type = rpki.ipaddrs.v4addr [static]

Type of underlying data (min and max).

De nition at line 178 of le resource_set.py.

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

- resource_set.py (2776)

10.144 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).

10.144.1 Detailed Description

Range of IPv6 addresses.

De nition at line 180 of le resource_set.py.

10.144.2 Member Data Documentation

10.144.2.1 rpki::resource_set.resource_range_ipv6::datum_type = rpki.ipaddrs.v6addr [static]

Type of underlying data (min and max).

De nition at line 188 of le resource_set.py.

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

- resource_set.py (2776)

10.145 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

10.145.1 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.

De nition at line 206 of le resource_set.py.

10.145.2 Member Function Documentation

10.145.2.1 def rpki.resource_set.resource_set.__init__(self, ini = None)

Initialize a resource_set.

De nition at line 219 of le resource_set.py.

10.145.2.2 def rpki.resource_set.resource_set.__str__(self)

Convert a resource_set to string format.

De nition at line 246 of le resource_set.py.

10.145.2.3 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.

De nition at line 255 of le resource_set.py.

10.145.2.4 def rpki.resource_set.resource_set.contains(self, item)

Set membership test for resource sets.

De nition at line 332 of le resource_set.py.

10.145.2.5 def rpki.resource_set.resource_set.difference(self, other)

Set difference for resource sets.

Definition at line 323 of file resource_set.py.

10.145.2.6 def rpki.resource_set.resource_set.from_sql(cls, sql, query, args= None)

Create resource set from an SQL query.

sql is an object that supports execute() and fetchall() methods like a DB API 2.0 cursor object.

query is an SQL query that returns a sequence of (min, max) pairs.

Definition at line 369 of file resource_set.py.

10.145.2.7 def rpki.resource_set.resource_set.intersection(self, other)

Set intersection for resource sets.

Definition at line 319 of file resource_set.py.

10.145.2.8 def rpki.resource_set.resource_set.issubset(self, other)

Test whether self is a subset (possibly improper) of other.

Definition at line 355 of file resource_set.py.

10.145.2.9 def rpki.resource_set.resource_set.issuperset(self, other)

Test whether self is a superset (possibly improper) of other.

Definition at line 364 of file resource_set.py.

10.145.2.10 def rpki.resource_set.resource_set.symmetric_difference(self, other)

Set symmetric difference (XOR) for resource sets.

Definition at line 327 of file resource_set.py.

10.145.2.11 def rpki.resource_set.resource_set.union(self, other)

Set union for resource sets.

Definition at line 288 of file resource_set.py.

10.145.3 Member Data Documentation

10.145.3.1 rpki::resource_set.resource_set::inherit = False [static]

Boolean indicating whether this resource_set uses RFC 3779 inheritance.

Reimplemented in rpki.resource_set.resource_set_as and rpki.resource_set.resource_set_ip.

Definition at line 217 of file resource_set.py.

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

- resource_set.py (2776)

10.146 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

10.146.1 Detailed Description

Autonomous System Number resource set.

De nition at line 384 of le resource_set.py.

10.146.2 Member Function Documentation

10.146.2.1 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.

De nition at line 404 of le resource_set.py.

10.146.2.2 def rpki.resource_set.resource_set_as.parse_str(self, x)

Parse ASN resource sets from text (eg, XML attributes).

De nition at line 394 of le resource_set.py.

10.146.2.3 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.

De nition at line 422 of le resource_set.py.

10.146.3 Member Data Documentation

10.146.3.1 rpki.resource_set.resource_set_as.inherit

Boolean indicating whether this resource_set uses RFC 3779 inheritance.

Reimplemented from rpki.resource_set.resource_set.

De nition at line 420 of le resource_set.py.

10.146.3.2 rpki::resource_set.resource_set_as::range_type = resource_range_as [static]

Type of range underlying this type of resource_set

De nition at line 392 of le resource_set.py.

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

- resource_set.py (2776)

10.147 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.

10.147.1 Detailed Description

(Generic) IP address resource set.

This is a virtual class. You probably don't want to use it directly.

De nition at line 434 of le resource_set.py.

10.147.2 Member Function Documentation

10.147.2.1 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.

De nition at line 454 of le resource_set.py.

10.147.2.2 def rpki.resource_set.resource_set_ip.parse_str(self, x)

Parse IP address resource sets from text (eg, XML attributes).

De nition at line 442 of le resource_set.py.

10.147.2.3 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.

De nition at line 472 of le resource_set.py.

10.147.3 Member Data Documentation

10.147.3.1 rpki.resource_set.resource_set_ip.inherit

Boolean indicating whether this resource_set uses RFC 3779 inheritance.

Reimplemented from rpki.resource_set.resource_set

De nition at line 470 of le resource_set.py.

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

- resource_set.py (2776)

10.148 rpki.resource_set.resource_set_ipv4 Class Reference

Inherits rpki::resource_set::resource_set_ip

Static Public Attributes

- string a = "\x00\x01"
  Address Family Identi er value for IPv4.
- range_type = resource_range_ipv4
  Type of range underlying this type of resource_set

10.148.1 Detailed Description

IPv4 address resource set.

De nition at line 484 of le resource_set.py.

10.148.2 Member Data Documentation

10.148.2.1 rpki::resource_set.resource_set_ipv4::a = "\x00\x01" [static]

Address Family Identi er value for IPv4.

De nition at line 497 of le resource_set.py.

10.148.2.2 rpki::resource_set.resource_set_ipv4::range_type = resource_range_ipv4 [static]

Type of range underlying this type of resource_set

De nition at line 492 of le resource_set.py.

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

- resource_set.py (2776)

10.149 rpki.resource_set.resource_set_ipv6 Class Reference

Inherits rpki::resource_set::resource_set_ip

Static Public Attributes

- string a = "\x00\x02"
  Address Family Identi er value for IPv6.
- range_type = resource_range_ipv6
  Type of range underlying this type of resource_set

10.149.1 Detailed Description

IPv6 address resource set.

De nition at line 499 of le resource_set.py.

10.149.2 Member Data Documentation

10.149.2.1 rpki::resource_set.resource_set_ipv6::a = "\x00\x02" [static]

Address Family Identi er value for IPv6.

De nition at line 512 of le resource_set.py.

10.149.2.2 rpki::resource_set.resource_set_ipv6::range_type = resource_range_ipv6 [static]

Type of range underlying this type of resource_set

De nition at line 507 of le resource_set.py.

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

- resource_set.py (2776)

10.150 rpki.resource_set.roa_pre x Class Reference

Inherits object.

Inherited by rpki.resource_set.roa_pre x_ipv4 and rpki.resource_set.roa_pre x_ipv6.

Public Member Functions

- def __cmp__
- def __init__
- def __str__
- def max
- def min
- def to_resource_range
- def to_roa_tuple

Public Attributes

- max_pre xlen

  Maxmimum pre x length.

- pre x

  The pre x itself, an IP address with bits beyond the pre x length zeroed.

- pre xlen

  (Minimum) pre x length.

10.150.1 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.

De nition at line 666 of le resource_set.py.

10.150.2 Member Function Documentation

10.150.2.1 def rpki.resource_set.roa_pre x.__cmp__(self, other)

Compare two ROA prefix objects. Comparision is based on prefix, prefixlen, and max_prefixlen, in that order.

De nition at line 697 of le resource_set.py.

10.150.2.2 def rpki.resource_set.roa_pre x.__init__ (self, pre x, pre xlen, max_pre xlen = None)

Initialize a ROA prefix. max_prefixlen is optional and defaults to prefixlen. max_prefixlen must not be smaller than prefixlen.

De nition at line 685 of le resource_set.py.

10.150.2.3 def rpki.resource_set.roa_pre x.__str__ (self)

Convert a ROA prefix to string format.

De nition at line 710 of le resource_set.py.

10.150.2.4 def rpki.resource_set.roa_pre x.max (self)

Return highest address covered by prefix.

De nition at line 731 of le resource_set.py.

10.150.2.5 def rpki.resource_set.roa_pre x.min (self)

Return lowest address covered by prefix.

De nition at line 727 of le resource_set.py.

10.150.2.6 def rpki.resource_set.roa_pre x.to_resource_range (self)

Convert this ROA prefix to the equivilent resource_range_ip object. This is an irreversable transformation because it loses the max_prefixlen attribute, nothing we can do about that.

De nition at line 719 of le resource_set.py.

10.150.2.7 def rpki.resource_set.roa_pre x.to_roa_tuple(self)

Convert a resource_range_ip to tuple format for ROA ASN.1 encoding.

De nition at line 738 of le resource_set.py.

10.150.3 Member Data Documentation

10.150.3.1 rpki::resource_set.roa_pre x::max_pre xlen

Maxmimum pre x length.

De nition at line 695 of le resource_set.py.

10.150.3.2 rpki::resource_set.roa_pre x::pre x

The pre x itself, an IP address with bits beyond the pre x length zeroed.

De nition at line 693 of le resource_set.py.

10.150.3.3 rpki::resource_set.roa_pre x::pre xlen

(Minimum) pre x length.

De nition at line 694 of le resource_set.py.

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

- resource_set.py (2776)

10.151 rpki.resource_set.roa_pre x_ipv4 Class Reference

Inherits rpki::resource_set::roa_pre x.

Static Public Attributes

- range_type = resource_range_ipv4
  Type of corresponding resource_range_ip

10.151.1 Detailed Description

IPv4 ROA prefix.

De nition at line 746 of le resource_set.py.

10.151.2 Member Data Documentation

10.151.2.1 rpki::resource_set.roa_pre x_ipv4::range_type = resource_range_ipv4 [static]

Type of corresponding resource_range_ip

De nition at line 754 of le resource_set.py.

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

- resource_set.py (2776)

10.152 rpki.resource_set.roa_pre x_ipv6 Class Reference

Inherits rpki::resource_set::roa_pre x

Static Public Attributes

- range_type = resource_range_ipv6
  Type of corresponding resource_range_ip

10.152.1 Detailed Description

IPv6 ROA prefix.

De nition at line 756 of le resource_set.py.

10.152.2 Member Data Documentation

10.152.2.1 rpki::resource_set.roa_pre x_ipv6::range_type = resource_range_ipv6 [static]

Type of corresponding resource_range_ip.

De nition at line 764 of le resource_set.py.

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

- resource_set.py (2776)

10.153 rpki.resource_set.roa_pre x_set Class Reference

Inherits list.

Inherited by rpki.resource_set.roa_pre x_set_ipv4, and rpki.resource_set.roa_pre x_set_ipv6.

Public Member Functions

- def __init__
- def __str__
- def from_sql
- def parse_str
- def to_resource_set
- def to_roa_tuple

10.153.1 Detailed Description

Set of ROA prefixes, analogous to the resource_set_ip class.

De nition at line 766 of le resource_set.py.

10.153.2 Member Function Documentation

10.153.2.1 def rpki.resource_set.roa_pre x_set.__init__(self, ini = None)

Initialize a ROA prefix set.

De nition at line 771 of le resource_set.py.

10.153.2.2 def rpki.resource_set.roa_pre x_set.__str__(self)

Convert a ROA prefix set to string format.

Definition at line 791 of file resource_set.py.

10.153.2.3 def rpki.resource_set.roa_pre x_set.from_sql(cls, sql, query, args = None)

Create ROA prefix set from an SQL query.

sql is an object that supports execute() and fetchall() methods like a DB API 2.0 cursor object.

query is an SQL query that returns a sequence of (prefix, prefixlen, max_prefixlen) triples.

Definition at line 825 of file resource_set.py.

10.153.2.4 def rpki.resource_set.roa_pre x_set.parse_str(self, x)

Parse ROA prefix from text (eg, an XML attribute).

Definition at line 795 of file resource_set.py.

10.153.2.5 def rpki.resource_set.roa_pre x_set.to_resource_set(self)

Convert a ROA prefix set to a resource set. This is an irreversable transformation. We have to compute a union here because ROA prefix sets can include overlaps, while RFC 3779 resource sets cannot. This is ugly, and there is almost certainly a more efficient way to do this, but start by getting the output right before worrying about making it fast or pretty.

Definition at line 807 of file resource_set.py.

10.153.2.6 def rpki.resource_set.roa_pre x_set.to_roa_tuples(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.

De nition at line 840 of le resource_set.py.

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

- resource_set.py (2776)

10.154 rpki.resource_set.roa_pre x_set_ipv4 Class Reference

Inherits rpki::resource_set::roa_pre x_set.

Static Public Attributes

- pre x_type = roa_pre x_ipv4
  Type of underlying roa_pre x.
- resource_set_type = resource_set_ipv4
  Type of corresponding resource_set_ip class.

10.154.1 Detailed Description

Set of IPv4 ROA prefixes.

De nition at line 850 of le resource_set.py.

10.154.2 Member Data Documentation

10.154.2.1 rpki::resource_set.roa_pre x_set_ipv4::pre x_type = roa_pre x_ipv4 [static]

Type of underlying roa_pre x.

De nition at line 858 of le resource_set.py.

10.154.2.2 rpki::resource_set.roa_pre x_set_ipv4::resource_set_type = resource_set_ipv4 [static]

Type of corresponding resource_set_ip class.

De nition at line 863 of le resource_set.py.

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

- resource_set.py (2776)

10.155 rpki.resource_set.roa_pre x_set_ipv6 Class Reference

Inherits rpki::resource_set::roa_pre x_set

Static Public Attributes

- pre x_type = roa_pre x_ipv6
  Type of underlying roa_pre x.
- resource_set_type = resource_set_ipv6
  Type of corresponding resource_set_ip class.

10.155.1 Detailed Description

Set of IPv6 ROA prefixes.

De nition at line 865 of le resource_set.py.

10.155.2 Member Data Documentation

10.155.2.1 rpki::resource_set.roa_pre x_set_ipv6::pre x_type = roa_pre x_ipv6 [static]

Type of underlying roa_pre x.

De nition at line 873 of le resource_set.py.

10.155.2.2 rpki::resource_set.roa_pre x_set_ipv6::resource_set_type = resource_set_ipv6 [static]

Type of corresponding resource_set_ip class.

De nition at line 878 of le resource_set.py.

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

- resource_set.py (2776)

10.156 rpki.roa.ROAIPAddress Class Reference

Inherits Sequence.

Public Member Functions

- def __init__

Public Attributes

- address
- maxLength

10.156.1 Detailed Description

De nition at line 47 of le roa.py.

10.156.2 Member Function Documentation

10.156.2.1 def rpki.roa.ROAIPAddress.__init__ (self, optional = 0, default = '')

De nition at line 48 of le roa.py.

10.156.3 Member Data Documentation

10.156.3.1 rpki.roa.ROAIPAddress.address

De nition at line 49 of le roa.py.

10.156.3.2 rpki.roa.ROAIPAddress.maxLength

De nition at line 50 of le roa.py.

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

- roa.py (2424)

10.157 rpki.roa.ROAIPAddresses Class Reference

InheritsSequenceOf

Public Member Functions

- def __init__

10.157.1 Detailed Description

De nition at line 54 of le roa.py.

10.157.2 Member Function Documentation

10.157.2.1 def rpki.roa.ROAIPAddresses.__init__(self, optional = 0, default = '')

De nition at line 55 of le roa.py.

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

- roa.py (2424)

10.158 rpki.roa.ROAIPAddressFamilies Class Reference

InheritsSequenceOf

Public Member Functions

- def __init__

10.158.1 Detailed Description

De nition at line 65 of le roa.py.

10.158.2 Member Function Documentation

10.158.2.1 def rpki.roa.ROAIPAddressFamilies.__init__ (self, optional = 0, default = '')

De nition at line 66 of le roa.py.

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

- roa.py (2424)

10.159 rpki.roa.ROAIPAddressFamily Class Reference

Inherits Sequence.

Public Member Functions

- def __init__

Public Attributes

- addresses
- addressFamily

10.159.1 Detailed Description

De nition at line 58 of le roa.py.

10.159.2 Member Function Documentation

10.159.2.1 def rpki.roa.ROAIPAddressFamily.__init__ (self, optional = 0, default = '')

De nition at line 59 of le roa.py.

10.159.3 Member Data Documentation

10.159.3.1 rpki.roa.ROAIPAddressFamily.addresses

De nition at line 61 of le roa.py.

10.159.3.2 rpki.roa.ROAIPAddressFamily.addressFamily

De nition at line 60 of le roa.py.

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

- roa.py (2424)

10.160 rpki.roa.RouteOriginAttestation Class Reference

InheritsSequence.

Public Member Functions

- def __init__

Public Attributes

- asID
- explicitVersion
- ipAddrBlocks
- version

10.160.1 Detailed Description

De nition at line 69 of le roa.py.

10.160.2 Member Function Documentation

10.160.2.1 def rpki.roa.RouteOriginAttestation.__init__ (self, optional = 0, default = ”)

De nition at line 70 of le roa.py.

10.160.3 Member Data Documentation

10.160.3.1 rpki.roa.RouteOriginAttestation.asID

De nition at line 73 of le roa.py.

10.160.3.2 rpki.roa.RouteOriginAttestation.explicitVersion

De nition at line 72 of le roa.py.

10.160.3.3 rpki.roa.RouteOriginAttestation.ipAddrBlocks

De nition at line 74 of le roa.py.

10.160.3.4 rpki.roa.RouteOriginAttestation.version

De nition at line 71 of le roa.py.

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

- roa.py (2424)

10.161 rpki.rpki_engine.ca_detail_obj Class Reference

Inheritsrpki::sql::sql_persistent

Public Member Functions

- def activate
- def ca
- def child_certs
- def create
- def crl_published_callback

- def crl_uri
- def crl_uri_tail
- def delete
- def generate_crl
- def generate_manifest
- def generate_manifest_cert
- def issue
- def issue_ee
- def manifest_published_callback
- def manifest_uri
- def revoke
- def revoked_certs
- def roas
- def sql_decode
- def update

Public Attributes

- ca_cert_uri
- ca_id
- gctx
- latest_crl
- latest_manifest
- latest_manifest_cert
- manifest_private_key_id
- manifest_public_key
- nextUpdate
- private_key_id
- public_key
- state

Static Public Attributes

- crl_published = None
- latest_ca_cert = None
- manifest_published = None
- tuple sql_template

10.161.1 Detailed Description

Internal CA detail object.

De nition at line 563 of le rpki_engine.py.

10.161.2 Member Function Documentation

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

Activate this ca_detail.

Definition at line 625 of file rpki_engine.py.

10.161.2.2 def rpki.rpki_engine.ca_detail_obj.ca(self)

Fetch CA object to which this ca_detail links.

Definition at line 597 of file rpki_engine.py.

10.161.2.3 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 601 of file rpki_engine.py.

10.161.2.4 def rpki.rpki_engine.ca_detail_obj.create(cls, ca)

Create a new ca_detail object for a specified CA.

Definition at line 763 of file rpki_engine.py.

10.161.2.5 def rpki.rpki_engine.ca_detail_obj.crl_published_callback(self, pdu)

Check result of CRL publication.

Definition at line 886 of file rpki_engine.py.

10.161.2.6 def rpki.rpki_engine.ca_detail_obj.crl_uri (self, ca)

Return publication URI for this ca_detail's CRL.

De nition at line 613 of le rpki_engine.py.

10.161.2.7 def rpki.rpki_engine.ca_detail_obj.crl_uri_tail (self)

Return tail (filename portion) of publication URI for this ca_detail's CRL.

De nition at line 617 of le rpki_engine.py.

10.161.2.8 def rpki.rpki_engine.ca_detail_obj.delete (self, ca, publisher, allow_failure = False)

Delete this ca_detail and all of the certs it issued.

If allow_failure is true, we clean up as much as we can but don't raise an exception.

De nition at line 650 of le rpki_engine.py.

10.161.2.9 def rpki.rpki_engine.ca_detail_obj.generate_crl (self, publisher, nextUpdate = None)

Generate a new CRL for this ca_detail. At the moment this is unconditional, that is, it is up to the caller to decide whether a new CRL is needed.

De nition at line 850 of le rpki_engine.py.

10.161.2.10 def rpki.rpki_engine.ca_detail_obj.generate_manifest (self, publisher, nextUpdate = None)

Generate a new manifest for this ca_detail.

De nition at line 894 of le rpki_engine.py.

10.161.2.11 def rpki.rpki_engine.ca_detail_obj.generate_manifest_cert(self, ca)

Generate a new manifest certificate for this ca_detail.

De nition at line 798 of le rpki_engine.py.

10.161.2.12 def rpki.rpki_engine.ca_detail_obj.issues(self, ca, child, subject_key, sia, resources, publisher, child_cert = None)

Issue a new certificate to a child. Optional child_cert argument specifies an existing child_cert object to update in place; if not specified, we create a new one. Returns the child_cert object containing the newly issued cert.

De nition at line 810 of le rpki_engine.py.

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

Issue a new EE certificate.

De nition at line 781 of le rpki_engine.py.

10.161.2.14 def rpki.rpki_engine.ca_detail_obj.manifest_published_callback (self, pdu)

Check result of manifest publication.

De nition at line 928 of le rpki_engine.py.

10.161.2.15 def rpki.rpki_engine.ca_detail_obj.manifest_uri(self, ca)

Return publication URI for this ca_detail's manifest.

De nition at line 621 of le rpki_engine.py.

10.161.2.16 def rpki.rpki_engine.ca_detail_obj.revoke(self, cb, eb)

Request revocation of all certificates whose SKI matches the key for this ca_detail.

Tasks:

- Request revocation of old keypair by parent.

- Revoke all child certs issued by the old keypair.

- Generate a final CRL, signed with the old keypair, listing all the revoked certs, with a next CRL time after the last cert or CRL signed by the old keypair will have expired.

- Generate a corresponding final manifest.

- Destroy old keypairs.

- Leave final CRL and manifest in place until their nextupdate time has passed.

De nition at line 674 of le rpki_engine.py.

10.161.2.17 def rpki.rpki_engine.ca_detail_obj.revoked_certs(self)

Fetch all revoked_cert objects that link to this ca_detail.

De nition at line 605 of le rpki_engine.py.

10.161.2.18 def rpki.rpki_engine.ca_detail_obj.roas(self)

Fetch all ROA objects that link to this ca_detail.

De nition at line 609 of le rpki_engine.py.

10.161.2.19 def rpki.rpki_engine.ca_detail_obj.sql_decode(self, vals)

Extra assertions for SQL decode of a ca_detail_obj.

Reimplemented from rpki.sql.sql_persistent

De nition at line 589 of le rpki_engine.py.

10.161.2.20 def rpki.rpki_engine.ca_detail_obj.update(self, parent, ca, rc, sia_uri_changed, old_resources, callback, errback)

Need to get a new certificate for this ca_detail and perhaps frob children of this ca_detail.

De nition at line 738 of le rpki_engine.py.

10.161.3 Member Data Documentation

10.161.3.1 rpki.rpki_engine.ca_detail_obj.ca_cert_uri

De nition at line 633 of le rpki_engine.py.

10.161.3.2 rpki.rpki_engine.ca_detail_obj.ca_id

De nition at line 769 of le rpki_engine.py.

10.161.3.3 rpki.rpki_engine.ca_detail_obj.crl_published = None[static]

De nition at line 585 of le rpki_engine.py.

10.161.3.4 rpki.rpki_engine.ca_detail_obj.gctx

Reimplemented from rpki.sql.sql_persistent

De nition at line 768 of le rpki_engine.py.

10.161.3.5 rpki.rpki_engine.ca_detail_obj.latest_ca_cert = None[static]

De nition at line 587 of le rpki_engine.py.

10.161.3.6 rpki.rpki_engine.ca_detail_obj.latest_crl

De nition at line 873 of le rpki_engine.py.

10.161.3.7 rpki.rpki_engine.ca_detail_obj.latest_manifest

De nition at line 914 of le rpki_engine.py.

10.161.3.8 rpki.rpki_engine.ca_detail_obj.latest_manifest_cert

De nition at line 731 of le rpki_engine.py.

10.161.3.9 rpki.rpki_engine.ca_detail_obj.manifest_private_key_id

De nition at line 729 of le rpki_engine.py.

10.161.3.10 rpki.rpki_engine.ca_detail_obj.manifest_public_key

De nition at line 730 of le rpki_engine.py.

10.161.3.11 rpki.rpki_engine.ca_detail_obj.manifest_published = None [static]

De nition at line 586 of le rpki_engine.py.

10.161.3.12 rpki.rpki_engine.ca_detail_obj.nextUpdate

De nition at line 707 of le rpki_engine.py.

10.161.3.13 rpki.rpki_engine.ca_detail_obj.private_key_id

De nition at line 728 of le rpki_engine.py.

10.161.3.14 rpki.rpki_engine.ca_detail_obj.public_key

De nition at line 773 of le rpki_engine.py.

10.161.3.15 tuple rpki.rpki_engine.ca_detail_obj.sql_template[static]

Initial value:

```
rpki.sql.template(
        "ca_detail",
        "ca_detail_id",
        ("private_key_id",                  rpki.x509.RSA),
        ("public_key",                        rpki.x509.RSApublic),
        ("latest_ca_cert",                  rpki.x509.X509),
        ("manifest_private_key_id",  rpki.x509.RSA),
        ("manifest_public_key",          rpki.x509.RSApublic),
        ("latest_manifest_cert",        rpki.x509.X509),
        ("latest_manifest",                rpki.x509.SignedManifest),
        ("latest_crl",                       rpki.x509.CRL),
        ("crl_published",                  rpki.sundial.datetime),
        ("manifest_published",          rpki.sundial.datetime),
        "state",
        "ca_cert_uri",
        "ca_id")
```

De nition at line 568 of le rpki_engine.py.

10.161.3.16 rpki.rpki_engine.ca_detail_obj.state

De nition at line 635 of le rpki_engine.py.

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

- rpki_engine.py (2934)

10.162 rpki.rpki_engine.ca_obj Class Reference

Inheritsrpki::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_issue_response_candidates
- def fetch_pending
- def fetch_revoked
- def next_crl_number
- def next_manifest_number
- def next_serial_number
- def parent
- def rekey
- def revoke

Public Attributes

- gctx
- parent_id
- parent_resource_class
- sia_uri

Static Public Attributes

- int last_crl_sn = 0
- int last_issued_sn = 0
- int last_manifest_sn = 0
- tuple sql_template

10.162.1 Detailed Description

Internal CA object.

De nition at line 309 of le rpki_engine.py.

10.162.2 Member Function Documentation

10.162.2.1 def rpki.rpki_engine.ca_obj.ca_details(self)

Fetch all ca_detail objects that link to this CA object.

Definition at line 331 of file rpki_engine.py.

10.162.2.2 def rpki.rpki_engine.ca_obj.check_for_updates(self, parent, rc, cb, eb)

Parent has signaled continued existance of a resource class we already knew about, so we need to check for an updated certificate, changes in resource coverage, revocation and reissue with the same key, etc.

Definition at line 372 of file rpki_engine.py.

10.162.2.3 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 359 of file rpki_engine.py.

10.162.2.4 def rpki.rpki_engine.ca_obj.create(cls, parent, rc, cb, eb)

Parent has signaled existance of a new resource class, so we need to create and set up a corresponding CA object.

Definition at line 452 of file rpki_engine.py.

10.162.2.5 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.

De nition at line 476 of le rpki_engine.py.

10.162.2.6 def rpki.rpki_engine.ca_obj.fetch_actives(self)

Fetch the active ca_detail for this CA, if any.

De nition at line 339 of le rpki_engine.py.

10.162.2.7 def rpki.rpki_engine.ca_obj.fetch_deprecateds(self)

Fetch deprecated ca_details for this CA, if any.

De nition at line 343 of le rpki_engine.py.

10.162.2.8 def rpki.rpki_engine.ca_obj.fetch_issue_response_candidates(self)

Fetch ca_details which are candidates for consideration when processing an up-down issue_response PDU.

De nition at line 351 of le rpki_engine.py.

10.162.2.9 def rpki.rpki_engine.ca_obj.fetch_pendings(self)

Fetch the pending ca_details for this CA, if any.

De nition at line 335 of le rpki_engine.py.

10.162.2.10 def rpki.rpki_engine.ca_obj.fetch_revokeds(self)

Fetch revoked ca_details for this CA, if any.

De nition at line 347 of le rpki_engine.py.

10.162.2.11 def rpki.rpki_engine.ca_obj.next_crl_number(self)

Allocate a CRL serial number.

De nition at line 518 of le rpki_engine.py.

10.162.2.12 def rpki.rpki_engine.ca_obj.next_manifest_numbers(self)

Allocate a manifest serial number.

De nition at line 510 of le rpki_engine.py.

10.162.2.13 def rpki.rpki_engine.ca_obj.next_serial_numbers(self)

Allocate a certificate serial number.

De nition at line 502 of le rpki_engine.py.

10.162.2.14 def rpki.rpki_engine.ca_obj.parent(self)

Fetch parent object to which this CA object links.

De nition at line 327 of le rpki_engine.py.

10.162.2.15 def rpki.rpki_engine.ca_obj.rekey(self, cb, eb)

Initiate a rekey operation for this ca. Generate a new keypair. Request cert from parent using new keypair. Mark result as our active ca_detail. Reissue all child certs issued by this ca using the new ca_detail.

De nition at line 526 of le rpki_engine.py.

10.162.2.16 def rpki.rpki_engine.ca_obj.revoke(self, cb, eb)

Revoke deprecated ca_detail objects associated with this ca.

De nition at line 551 of le rpki_engine.py.

10.162.3 Member Data Documentation

10.162.3.1 rpki.rpki_engine.ca_obj.gctx

Reimplemented from rpki.sql.sql_persistent

De nition at line 459 of le rpki_engine.py.

10.162.3.2 int rpki.rpki_engine.ca_obj.last_crl_sn = 0 [static]

De nition at line 323 of le rpki_engine.py.

10.162.3.3 int rpki.rpki_engine.ca_obj.last_issued_sn = 0 [static]

De nition at line 324 of le rpki_engine.py.

10.162.3.4 int rpki.rpki_engine.ca_obj.last_manifest_sn = 0 [static]

De nition at line 325 of le rpki_engine.py.

10.162.3.5 rpki.rpki_engine.ca_obj.parent_id

De nition at line 460 of le rpki_engine.py.

10.162.3.6 rpki.rpki_engine.ca_obj.parent_resource_class

De nition at line 461 of le rpki_engine.py.

10.162.3.7 rpki.rpki_engine.ca_obj.sia_uri

De nition at line 383 of le rpki_engine.py.

10.162.3.8 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")
```

De nition at line 314 of le rpki_engine.py.

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

- rpki_engine.py (2934)

10.163 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 published_callback
- def reissue
- def revoke
- def uri
- def uri_tail

Public Attributes

- ca_detail_id
- cert
- child_id
- gctx
- published

Static Public Attributes

- tuple sql_template

10.163.1 Detailed Description

Certificate that has been issued to a child.

De nition at line 937 of le rpki_engine.py.

10.163.2 Member Function Documentation

10.163.2.1 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.

De nition at line 951 of le rpki_engine.py.

10.163.2.2 def rpki.rpki_engine.child_cert_obj.ca_detail (self)

Fetch ca_detail object to which this child_cert object links.

De nition at line 968 of le rpki_engine.py.

10.163.2.3 def rpki.rpki_engine.child_cert_obj.child (self)

Fetch child object to which this child_cert object links.

Definition at line 964 of file rpki_engine.py.

10.163.2.4 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 1049 of file rpki_engine.py.

10.163.2.5 def rpki.rpki_engine.child_cert_obj.published_callback (self, pdu)

Publication callback: check result and mark published.

Definition at line 1081 of file rpki_engine.py.

10.163.2.6 def rpki.rpki_engine.child_cert_obj.reissue (self, ca_detail, publisher, resources = None, sia = None)

Reissue an existing child cert, reusing the public key. If the child cert we would generate is identical to the one we already have, we just return the one we already have. If we have to revoke the old child cert when generating the new one, we have to generate a new child_cert_obj, so calling code that needs the updated child_cert_obj must use the return value from this method.

Definition at line 992 of file rpki_engine.py.

10.163.2.7 def rpki.rpki_engine.child_cert_obj.revoke (self, publisher)

Revoke a child cert.

Definition at line 980 of file rpki_engine.py.

10.163.2.8 def rpki.rpki_engine.child_cert_obj.uri (self, ca)

Return the publication URI for this child_cert.

De nition at line 976 of le rpki_engine.py.

10.163.2.9 def rpki.rpki_engine.child_cert_obj.uri_tail (self)

Return the tail (filename) portion of the URI for this child_cert.

De nition at line 972 of le rpki_engine.py.

10.163.3 Member Data Documentation

10.163.3.1 rpki.rpki_engine.child_cert_obj.ca_detail_id

De nition at line 958 of le rpki_engine.py.

10.163.3.2 rpki.rpki_engine.child_cert_obj.cert

De nition at line 959 of le rpki_engine.py.

10.163.3.3 rpki.rpki_engine.child_cert_obj.child_id

De nition at line 957 of le rpki_engine.py.

10.163.3.4 rpki.rpki_engine.child_cert_obj.gctx

Reimplemented from rpki.sql.sql_persistent

De nition at line 956 of le rpki_engine.py.

10.163.3.5 rpki.rpki_engine.child_cert_obj.published

De nition at line 960 of le rpki_engine.py.

10.163.3.6 tuple rpki.rpki_engine.child_cert_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
        "child_cert",
        "child_cert_id",
        ("cert",  rpki.x509.X509),
        "child_id",
        "ca_detail_id",
        "ski",
        ("published",  rpki.sundial.datetime))
```

De nition at line 942 of le rpki_engine.py.

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

- rpki_engine.py (2934)

10.164 rpki.rpki_engine.publication_queue Class Reference

Inheritsobject

Public Member Functions

- def __init__
- def call_pubd
- def publish
- def withdraw

Public Attributes

- handlers
- msgs
- repositories
- uris

Static Public Attributes

- replace= True

Private Member Functions

- def _add

10.164.1 Detailed Description

Utility to simplify publication from within rpkid.

General idea here is to accumulate a collection of objects to be published, in one or more repositories, each potentially with its own completion callback. Eventually we want to publish everything we've accumulated, at which point we need to iterate over the collection and do repository.call_pubd() for each repository.

De nition at line 1367 of le rpki_engine.py.

10.164.2 Member Function Documentation

10.164.2.1 def rpki.rpki_engine.publication_queue.__init__(self)

De nition at line 1380 of le rpki_engine.py.

10.164.2.2 def rpki.rpki_engine.publication_queue._add(self, cls, uri, obj, repository, handler, withdraw) [private]

De nition at line 1387 of le rpki_engine.py.

10.164.2.3 def rpki.rpki_engine.publication_queue.call_pubd(self, cb, eb)

De nition at line 1410 of le rpki_engine.py.

10.164.2.4 def rpki.rpki_engine.publication_queue.publish(self, cls, uri, obj, repository, handler = None)

De nition at line 1404 of le rpki_engine.py.

10.164.2.5 def rpki.rpki_engine.publication_queue.withdraw (self, cls, uri, obj, repository, handler = None)

De nition at line 1407 of le rpki_engine.py.

10.164.3 Member Data Documentation

10.164.3.1 rpki.rpki_engine.publication_queue.handlers

De nition at line 1383 of le rpki_engine.py.

10.164.3.2 rpki.rpki_engine.publication_queue.msgs

De nition at line 1382 of le rpki_engine.py.

10.164.3.3 rpki.rpki_engine.publication_queue.replace = True [static]

De nition at line 1378 of le rpki_engine.py.

10.164.3.4 rpki.rpki_engine.publication_queue.repositories

De nition at line 1381 of le rpki_engine.py.

10.164.3.5 rpki.rpki_engine.publication_queue.uris

De nition at line 1385 of le rpki_engine.py.

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

- rpki_engine.py (2934)

10.165 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

10.165.1 Detailed Description

Tombstone for a revoked certificate.

Definition at line 1089 of file rpki_engine.py.

10.165.2 Member Function Documentation

10.165.2.1 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 1102 of file rpki_engine.py.

10.165.2.2 def rpki.rpki_engine.revoked_cert_obj.ca_details(self)

Fetch ca_detail object to which this revoked_cert_obj links.

De nition at line 1113 of le rpki_engine.py.

10.165.2.3 def rpki.rpki_engine.revoked_cert_obj.revoke(cls, cert, ca_detail)

Revoke a certificate.

De nition at line 1118 of le rpki_engine.py.

10.165.3 Member Data Documentation

10.165.3.1 rpki.rpki_engine.revoked_cert_obj.ca_detail_id

De nition at line 1109 of le rpki_engine.py.

10.165.3.2 rpki.rpki_engine.revoked_cert_obj.expires

De nition at line 1108 of le rpki_engine.py.

10.165.3.3 rpki.rpki_engine.revoked_cert_obj.gctx

Reimplemented from rpki.sql.sql_persistent
De nition at line 1105 of le rpki_engine.py.

10.165.3.4 rpki.rpki_engine.revoked_cert_obj.revoked

De nition at line 1107 of le rpki_engine.py.

10.165.3.5 rpki.rpki_engine.revoked_cert_obj.serial

De nition at line 1106 of le rpki_engine.py.

10.165.3.6 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))
```

De nition at line 1094 of le rpki_engine.py.

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

- rpki_engine.py (2934)

10.166 rpki.rpki_engine.roa_obj Class Reference

Inherits rpki::sql::sql_persistent

Public Member Functions

- def __init__
- def ca_detail
- def generate
- def published_callback
- def regenerate
- def revoke
- def self
- def sql_delete_hook
- def sql_fetch_hook
- def sql_insert_hook
- def update
- def uri
- def uri_tail

Public Attributes

- asn
- gctx
- ipv4
- ipv6
- self_id

Static Public Attributes

- ca_detail_id = None
- cert = None
- published = None
- roa = None
- tuple sql_template

10.166.1 Detailed Description

Route Origin Authorization.

De nition at line 1129 of le rpki_engine.py.

10.166.2 Member Function Documentation

10.166.2.1 def rpki.rpki_engine.roa_obj.__init__ (self, gctx = None, self_id = None, asn = None, ipv4 = None, ipv6 = None)

De nition at line 1195 of le rpki_engine.py.

10.166.2.2 def rpki.rpki_engine.roa_obj.ca_detail (self)

Fetch ca_detail object to which this roa_obj links.

De nition at line 1155 of le rpki_engine.py.

10.166.2.3 def rpki.rpki_engine.roa_obj.generate (self, publisher)

Generate a ROA.

At present this does not support ROAs with multiple signatures (neither does the current CMS code).

At present we have no way of performing a direct lookup from a desired set of resources to a covering certificate, so we have to search. This could be quite slow if we have a lot of active ca_detail objects. Punt on the issue for now, revisit if profiling shows this as a hotspot.

Once we have the right covering certificate, we generate the ROA payload, generate a new EE certificate, use the EE certificate to sign the ROA payload, publish the result, then throw away the private key for the EE cert, all per the ROA specification. This implies that generating a lot of ROAs will tend to thrash /dev/random, but there is not much we can do about that.

De nition at line 1238 of le rpki_engine.py.

10.166.2.4 def rpki.rpki_engine.roa_obj.published_callback (self, pdu)

Check publication result.

De nition at line 1304 of le rpki_engine.py.

10.166.2.5 def rpki.rpki_engine.roa_obj.regenerate (self, publisher)

Reissue ROA associated with this roa_obj.

De nition at line 1344 of le rpki_engine.py.

10.166.2.6 def rpki.rpki_engine.roa_obj.revoke (self, publisher, regenerate= False , allow_failure = False)

Withdraw ROA associated with this roa_obj.

In order to preserve make-before-break properties without

duplicating code, this method also handles generating a replacement ROA when requested.

If allow_failure is set, failing to withdraw the ROA will not be considered an error.

De nition at line 1312 of le rpki_engine.py.

10.166.2.7 def rpki.rpki_engine.roa_obj.self (self)

Fetch self object to which this roa_obj links.

De nition at line 1149 of le rpki_engine.py.

10.166.2.8 def rpki.rpki_engine.roa_obj.sql_delete_hooks (self)

Extra SQL delete actions for roa_obj -- handle prefix lists.

Reimplemented from rpki.sql.sql_persistent

De nition at line 1189 of le rpki_engine.py.

10.166.2.9 def rpki.rpki_engine.roa_obj.sql_fetch_hooks (self)

Extra SQL fetch actions for roa_obj -- handle prefix lists.

Reimplemented from rpki.sql.sql_persistent

De nition at line 1161 of le rpki_engine.py.

10.166.2.10 def rpki.rpki_engine.roa_obj.sql_insert_hooks (self)

Extra SQL insert actions for roa_obj -- handle prefix lists.

Reimplemented from rpki.sql.sql_persistent

De nition at line 1175 of le rpki_engine.py.

10.166.2.11 def rpki.rpki_engine.roa_obj.update (self, publisher)

Bring this roa_obj's ROA up to date if necesssary.

De nition at line 1208 of le rpki_engine.py.

10.166.2.12 def rpki.rpki_engine.roa_obj.uri (self, key = None)

Return the publication URI for this roa_obj's ROA.

De nition at line 1353 of le rpki_engine.py.

10.166.2.13 def rpki.rpki_engine.roa_obj.uri_tail (self, key = None)

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

De nition at line 1359 of le rpki_engine.py.

10.166.3 Member Data Documentation

10.166.3.1 rpki.rpki_engine.roa_obj.asn

De nition at line 1199 of le rpki_engine.py.

10.166.3.2 rpki.rpki_engine.roa_obj.ca_detail_id = None [static]

De nition at line 1144 of le rpki_engine.py.

10.166.3.3 rpki.rpki_engine.roa_obj.cert = None [static]

De nition at line 1145 of le rpki_engine.py.

10.166.3.4 rpki.rpki_engine.roa_obj.gctx

Reimplemented from rpki.sql.sql_persistent

De nition at line 1197 of le rpki_engine.py.

10.166.3.5 rpki.rpki_engine.roa_obj.ipv4

De nition at line 1200 of le rpki_engine.py.

10.166.3.6 rpki.rpki_engine.roa_obj.ipv6

De nition at line 1201 of le rpki_engine.py.

10.166.3.7 rpki.rpki_engine.roa_obj.published = None [static]

De nition at line 1147 of le rpki_engine.py.

10.166.3.8 rpki.rpki_engine.roa_obj.roa = None [static]

De nition at line 1146 of le rpki_engine.py.

10.166.3.9 rpki.rpki_engine.roa_obj.self_id

De nition at line 1198 of le rpki_engine.py.

10.166.3.10 tuple rpki.rpki_engine.roa_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
        "roa",
        "roa_id",
        "ca_detail_id",
```

```
"self_id",
"asn",
("roa",  rpki.x509.ROA),
("cert",  rpki.x509.X509),
("published",  rpki.sundial.datetime))
```

De nition at line 1134 of le rpki_engine.py.

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

- rpki_engine.py (2934)

10.167 rpki.rpki_engine.rpkid_context Class Reference

Inheritsobject

Public Member Functions

- def __init__
- def build_https_ta_cache
- def checkpoint
- def clear_https_ta_cache
- def cron
- def cronjob_handler
- def irdb_query
- def irdb_query_child_resources
- def irdb_query_roa_requests
- def left_right_handler
- def start_cron
- def up_down_handler

Public Attributes

- bpki_ta
- cron_keepalive
- cron_period
- cron_timeout
- cron_timer
- https_server_host
- https_server_port
- initial_delay
- irbe_cert
- irdb_cert

- irdb_url
- publication_kludge_base
- rpkid_cert
- rpkid_key
- sql
- use_internal_cron

Static Public Attributes

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

10.167.1 Detailed Description

A container for various global rpkid parameters.

Definition at line 39 of file rpki_engine.py.

10.167.2 Member Function Documentation

10.167.2.1 def rpki.rpki_engine.rpkid_context.__init__ (self, cfg)

Definition at line 44 of file rpki_engine.py.

10.167.2.2 def rpki.rpki_engine.rpkid_context.build_https_ta_cache (self)

Build dynamic TLS trust anchors.

Definition at line 289 of file rpki_engine.py.

10.167.2.3 def rpki.rpki_engine.rpkid_context.checkpoint (self)

Record that we were still alive when we got here, by resetting keepalive timer.

Definition at line 200 of file rpki_engine.py.

10.167.2.4 def rpki.rpki_engine.rpkid_context.clear_https_ta_caches(self)

Clear dynamic TLS trust anchors.

De nition at line 280 of le rpki_engine.py.

10.167.2.5 def rpki.rpki_engine.rpkid_context.cron (self, cb = None)

Periodic tasks.

De nition at line 208 of le rpki_engine.py.

10.167.2.6 def rpki.rpki_engine.rpkid_context.cronjob_handler (self, query, path, cb)

External trigger for periodic tasks. This is somewhat obsolete now that we have internal timers, but the test framework still uses it.

De nition at line 264 of le rpki_engine.py.

10.167.2.7 def rpki.rpki_engine.rpkid_context.irdb_query (self, q_pdu, callback, errback)

Perform an IRDB callback query.

De nition at line 86 of le rpki_engine.py.

10.167.2.8 def rpki.rpki_engine.rpkid_context.irdb_query_child_resources (self, self_handle, child_handle, callback, errback)

Ask IRDB about a child's resources.

De nition at line 112 of le rpki_engine.py.

10.167.2.9 def rpki.rpki_engine.rpkid_context.irdb_query_roa_requests (self, self_handle, callback, errback)

Ask IRDB about self's ROA requests.

De nition at line 134 of le rpki_engine.py.

10.167.2.10 def rpki.rpki_engine.rpkid_context.left_right_handler (self, query, path, cb)

Process one left-right PDU.

De nition at line 146 of le rpki_engine.py.

10.167.2.11 def rpki.rpki_engine.rpkid_context.start_cron (self)

Start clock for rpkid's internal cron process.

De nition at line 73 of le rpki_engine.py.

10.167.2.12 def rpki.rpki_engine.rpkid_context.up_down_handler (self, query, path, cb)

Process one up-down PDU.

De nition at line 172 of le rpki_engine.py.

10.167.3 Member Data Documentation

10.167.3.1 rpki.rpki_engine.rpkid_context.bpki_ta

De nition at line 48 of le rpki_engine.py.

10.167.3.2 rpki.rpki_engine.rpkid_context.cron_keepalive

De nition at line 68 of le rpki_engine.py.

10.167.3.3 rpki.rpki_engine.rpkid_context.cron_period

De nition at line 67 of le rpki_engine.py.

10.167.3.4 rpki.rpki_engine.rpkid_context.cron_timeout

De nition at line 71 of le rpki_engine.py.

10.167.3.5 rpki.rpki_engine.rpkid_context.cron_timer

De nition at line 79 of le rpki_engine.py.

10.167.3.6 rpki.rpki_engine.rpkid_context.https_server_host

De nition at line 56 of le rpki_engine.py.

10.167.3.7 rpki.rpki_engine.rpkid_context.https_server_port

De nition at line 57 of le rpki_engine.py.

10.167.3.8 rpki::rpki_engine.rpkid_context::https_ta_cache = None [static]

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

De nition at line 278 of le rpki_engine.py.

10.167.3.9 rpki.rpki_engine.rpkid_context.initial_delay

De nition at line 63 of le rpki_engine.py.

10.167.3.10 rpki.rpki_engine.rpkid_context.irbe_cert

De nition at line 50 of le rpki_engine.py.

10.167.3.11 rpki.rpki_engine.rpkid_context.irdb_cert

De nition at line 49 of le rpki_engine.py.

10.167.3.12 rpki.rpki_engine.rpkid_context.irdb_url

De nition at line 54 of le rpki_engine.py.

10.167.3.13 rpki.rpki_engine.rpkid_context.publication_kludge_base

De nition at line 59 of le rpki_engine.py.

10.167.3.14 rpki.rpki_engine.rpkid_context.rpkid_cert

De nition at line 51 of le rpki_engine.py.

10.167.3.15 rpki.rpki_engine.rpkid_context.rpkid_key

De nition at line 52 of le rpki_engine.py.

10.167.3.16 rpki.rpki_engine.rpkid_context.sql

De nition at line 46 of le rpki_engine.py.

10.167.3.17 tuple rpki.rpki_engine.rpkid_context.up_down_url_regexp = re.compile("/up-down/([-A-Z0-9_]+)/([-A-Z0-9_]+)$", re.I) [static]

De nition at line 170 of le rpki_engine.py.

10.167.3.18 rpki.rpki_engine.rpkid_context.use_internal_cron

De nition at line 61 of le rpki_engine.py.

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

- rpki_engine.py (2934)

10.168 rpki.sql.session Class Reference

Inheritsobject

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

10.168.1 Detailed Description

SQL session layer.

De nition at line 50 of le sql.py.

10.168.2 Member Function Documentation

10.168.2.1 def rpki.sql.session.__init__(self, cfg)

De nition at line 57 of le sql.py.

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

De nition at line 88 of le sql.py.

10.168.2.3 def rpki.sql.session.assert_pristine(self)

Assert that there are no dirty objects in the cache.

De nition at line 112 of le sql.py.

10.168.2.4 def rpki.sql.session.cache_clear(self)

Clear the object cache.

De nition at line 108 of le sql.py.

10.168.2.5 def rpki.sql.session.close(self)

De nition at line 77 of le sql.py.

10.168.2.6 def rpki.sql.session.connect(self)

De nition at line 72 of le sql.py.

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

De nition at line 96 of le sql.py.

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

De nition at line 99 of le sql.py.

10.168.2.9 def rpki.sql.session.fetchall(self)

De nition at line 102 of le sql.py.

10.168.2.10 def rpki.sql.session.lastrowids(self)

De nition at line 105 of le sql.py.

10.168.2.11 def rpki.sql.session.pings(self)

De nition at line 85 of le sql.py.

10.168.2.12 def rpki.sql.session.sweep(self)

Write any dirty objects out to SQL.

De nition at line 116 of le sql.py.

10.168.3 Member Data Documentation

10.168.3.1 rpki.sql.session._exceptions_enabled = False [static, private]

De nition at line 55 of le sql.py.

10.168.3.2 rpki.sql.session.cache

De nition at line 67 of le sql.py.

10.168.3.3 rpki.sql.session.cur

De nition at line 74 of le sql.py.

10.168.3.4 rpki.sql.session.database

De nition at line 64 of le sql.py.

10.168.3.5 rpki.sql.session.db

De nition at line 73 of le sql.py.

10.168.3.6 rpki.sql.session.dirty

De nition at line 68 of le sql.py.

10.168.3.7 rpki.sql.session.password

De nition at line 65 of le sql.py.

10.168.3.8 rpki.sql.session.username

De nition at line 63 of le sql.py.

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

- sql.py (2895)

10.169 rpki.sql.sql_persistent Class Reference

Inherits object.

Inherited by rpki.left_right.data_elt, rpki.publication.control_elt, rpki.rpki_engine.ca_-detail_obj, rpki.rpki_engine.ca_obj, rpki.rpki_engine.child_cert_obj, rpki.rpki_-engine.revoked_cert_obj, and rpki.rpki_engine.roa_obj.

Public Member Functions

- def sql_decode
- def sql_delete
- def sql_delete_hook
- def sql_encode

- def sql_fetch
- def sql_fetch_all
- def sql_fetch_hook
- def sql_fetch_where
- def sql_fetch_where1
- def sql_init
- def sql_insert_hook
- def sql_is_dirty
- def sql_mark_clean
- def sql_mark_deleted
- def sql_mark_dirty
- def sql_store
- def sql_update_hook

Public Attributes

- gctx

Static Public Attributes

- sql_debug = False
  Enable logging of SQL actions.
- sql_deleted = False
  Whether our cached copy of this object has been deleted.
- sql_in_db = False
  Whether this object is already in SQL or not.

10.169.1 Detailed Description

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

De nition at line 152 of le sql.py.

10.169.2 Member Function Documentation

10.169.2.1 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.

De nition at line 322 of le sql.py.

10.169.2.2 def rpki.sql.sql_persistent.sql_delete(self)

Delete this object from SQL.

De nition at line 293 of le sql.py.

10.169.2.3 def rpki.sql.sql_persistent.sql_delete_hook(self)

Customization hook.

Reimplemented in rpki.rpki_engine.roa_obj.

De nition at line 348 of le sql.py.

10.169.2.4 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.

De nition at line 309 of le sql.py.

10.169.2.5 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.

De nition at line 173 of le sql.py.

10.169.2.6 def rpki.sql.sql_persistent.sql_fetch_all(cls, gctx)

Fetch all objects of this type from SQL.

De nition at line 211 of le sql.py.

10.169.2.7 def rpki.sql.sql_persistent.sql_fetch_hook(cls, self)

Customization hook.

Reimplemented in rpki.rpki_engine.roa_obj

De nition at line 335 of le sql.py.

10.169.2.8 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.

De nition at line 216 of le sql.py.

10.169.2.9 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.

De nition at line 196 of le sql.py.

10.169.2.10 def rpki.sql.sql_persistent.sql_init(cls, gctx, row, key)

Initialize one Python object from the result of a SQL query.

De nition at line 243 of le sql.py.

10.169.2.11 def rpki.sql.sql_persistent.sql_insert_hook(self)

Customization hook.

Reimplemented in rpki.rpki_engine.roa_obj

De nition at line 339 of le sql.py.

10.169.2.12 def rpki.sql.sql_persistent.sql_is_dirty(self)

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

De nition at line 263 of le sql.py.

10.169.2.13 def rpki.sql.sql_persistent.sql_mark_clean(self)

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

De nition at line 259 of le sql.py.

10.169.2.14 def rpki.sql.sql_persistent.sql_mark_deleted(self)

Mark this object as needing to be deleted in SQL.

De nition at line 267 of le sql.py.

10.169.2.15 def rpki.sql.sql_persistent.sql_mark_dirty(self)

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

De nition at line 255 of le sql.py.

10.169.2.16 def rpki.sql.sql_persistent.sql_store(self)

Store this object to SQL.

De nition at line 271 of le sql.py.

10.169.2.17 def rpki.sql.sql_persistent.sql_update_hook(self)

Customization hook.

De nition at line 343 of le sql.py.

10.169.3 Member Data Documentation

10.169.3.1 rpki.sql.sql_persistent.gctx

Reimplemented in rpki.rpki_engine.ca_obj, rpki.rpki_engine.ca_detail_obj, rpki.rpki_engine.child_cert_obj, rpki.rpki_engine.revoked_cert_obj, and rpki.rpki_engine.roa_obj

De nition at line 248 of le sql.py.

10.169.3.2 rpki::sql.sql_persistent::sql_debug = False[static]

Enable logging of SQL actions.

De nition at line 170 of le sql.py.

10.169.3.3 rpki::sql.sql_persistent::sql_deleted = False [static]

Whether our cached copy of this object has been deleted.

De nition at line 165 of le sql.py.

10.169.3.4 rpki::sql.sql_persistent::sql_in_db = False [static]

Whether this object is already in SQL or not.

De nition at line 160 of le sql.py.

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

- sql.py (2895)

10.170 rpki.sql.template Class Reference

Inherits object.

Public Member Functions

- def __init__

Public Attributes

- columns
- delete
- index
- insert
- map
- select
- table
- update

10.170.1 Detailed Description

SQL template generator.

De nition at line 128 of le sql.py.

10.170.2 Member Function Documentation

10.170.2.1 def rpki.sql.template.__init__ (self, table_name, index_column, data_columns)

Build a SQL template.

Definition at line 133 of file sql.py.

10.170.3 Member Data Documentation

10.170.3.1 rpki.sql.template.columns

Definition at line 140 of file sql.py.

10.170.3.2 rpki.sql.template.delete

Definition at line 150 of file sql.py.

10.170.3.3 rpki.sql.template.index

Definition at line 139 of file sql.py.

10.170.3.4 rpki.sql.template.insert

Definition at line 143 of file sql.py.

10.170.3.5 rpki.sql.template.map

Definition at line 141 of file sql.py.

10.170.3.6 rpki.sql.template.select

De nition at line 142 of le sql.py.

10.170.3.7 rpki.sql.template.table

De nition at line 138 of le sql.py.

10.170.3.8 rpki.sql.template.update

De nition at line 146 of le sql.py.

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

- sql.py (2895)

10.171 rpki.sundial.datetime Class Reference

Inheritspydatetime::datetime

Public Member Functions

- def __add__
- def __radd__
- def __rsub__
- def __str__
- def __sub__
- def earlier
- def from_sql
- def fromASN1tuple
- def fromdatetime
- def fromGeneralizedTime
- def fromUTCTime
- def fromXMLtime
- def later
- def to_sql
- def toASN1tuple
- def toGeneralizedTime

- def totimestamp
- def toUTCTime
- def toXMLtime

Static Public Attributes

- tuple PKIX_threshhold = pydatetime.datetime(2050, 1, 1)

  Threshold speci ed in RFC 3280 for switchover from UTCTime to GeneralizedTime.

10.171.1 Detailed Description

RPKI extensions to standard datetime.datetime class. All work here is in UTC, so we use naive datetime objects.

De nition at line 54 of le sundial.py.

10.171.2 Member Function Documentation

10.171.2.1 def rpki.sundial.datetime.__add__(x, y)

De nition at line 163 of le sundial.py.

10.171.2.2 def rpki.sundial.datetime.__radd__(x, y)

De nition at line 164 of le sundial.py.

10.171.2.3 def rpki.sundial.datetime.__rsub__(x, y)

De nition at line 165 of le sundial.py.

10.171.2.4 def rpki.sundial.datetime.__str__(self)

De nition at line 124 of le sundial.py.

10.171.2.5 def rpki.sundial.datetime.__sub__(x, y)

De nition at line 166 of le sundial.py.

10.171.2.6 def rpki.sundial.datetime.earlier (self, other)

Return the earlier of two timestamps.

De nition at line 159 of le sundial.py.

10.171.2.7 def rpki.sundial.datetime.from_sql (cls, x)

Convert from SQL storage format.

De nition at line 136 of le sundial.py.

10.171.2.8 def rpki.sundial.datetime.fromASN1tuple (cls, x)

Convert from ASN.1 tuple representation.

De nition at line 86 of le sundial.py.

10.171.2.9 def rpki.sundial.datetime.fromdatetime (cls, x)

Convert a datetime.datetime object into this subclass. This is whacky due to the weird constructors for datetime.

De nition at line 128 of le sundial.py.

10.171.2.10 def rpki.sundial.datetime.fromGeneralizedTime (cls, x)

Convert from ASN.1 GeneralizedTime.

De nition at line 77 of le sundial.py.

10.171.2.11 def rpki.sundial.datetime.fromUTCTime (cls, x)

Convert from ASN.1 UTCTime.

De nition at line 68 of le sundial.py.

10.171.2.12 def rpki.sundial.datetime.fromXMLtime (cls, x)

Convert from XML time representation.

De nition at line 111 of le sundial.py.

10.171.2.13 def rpki.sundial.datetime.later (self, other)

Return the later of two timestamps.

De nition at line 155 of le sundial.py.

10.171.2.14 def rpki.sundial.datetime.to_sql (self)

Convert to SQL storage format.

There's something whacky going on in the MySQLdb module, it throws range errors when storing a derived type into a DATETIME column. Investigate some day, but for now brute force this by copying the relevant fields into a datetime.datetime for MySQLdb's consumption.

De nition at line 140 of le sundial.py.

10.171.2.15 def rpki.sundial.datetime.toASN1tuple (self)

Convert to ASN.1 tuple representation.

De nition at line 101 of le sundial.py.

10.171.2.16 def rpki.sundial.datetime.toGeneralizedTime(self)

Convert to ASN.1 GeneralizedTime.

De nition at line 81 of le sundial.py.

10.171.2.17 def rpki.sundial.datetime.totimestamp(self)

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

De nition at line 60 of le sundial.py.

10.171.2.18 def rpki.sundial.datetime.toUTCTime(self)

Convert to ASN.1 UTCTime.

De nition at line 72 of le sundial.py.

10.171.2.19 def rpki.sundial.datetime.toXMLtime(self)

Convert to XML time representation.

De nition at line 120 of le sundial.py.

10.171.3 Member Data Documentation

10.171.3.1 rpki::sundial.datetime::PKIX_threshhold = pydatetime.datetime(2050, 1, 1) [static]

Threshold speci ed in RFC 3280 for switchover from UTCTime to GeneralizedTime.

De nition at line 99 of le sundial.py.

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

- sundial.py (2785)

10.172 rpki.sundial.timedelta Class Reference

Inherits pydatetime::timedelta

Public Member Functions

- def __abs__
- def __add__
- def __div__
- def __ oordiv__
- def __mul__
- def __neg__
- def __pos__
- def __radd__
- def __rdiv__
- def __r oordiv__
- def __rmul__
- def __rsub__
- def __sub__
- def convert_to_seconds
- def fromtimedelta
- def parse

Static Public Attributes

- tuple regexp

  Hideously ugly regular expression to parse the complex text form.

10.172.1 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".

De nition at line 168 of le sundial.py.

10.172.2 Member Function Documentation

10.172.2.1 def rpki.sundial.timedelta.__abs__(x)

De nition at line 218 of le sundial.py.

10.172.2.2 def rpki.sundial.timedelta.__add__(x, y)

De nition at line 219 of le sundial.py.

10.172.2.3 def rpki.sundial.timedelta.__div__(x, y)

De nition at line 220 of le sundial.py.

10.172.2.4 def rpki.sundial.timedelta.__ oordiv__ (x, y)

De nition at line 221 of le sundial.py.

10.172.2.5 def rpki.sundial.timedelta.__mul__(x, y)

De nition at line 222 of le sundial.py.

10.172.2.6 def rpki.sundial.timedelta.__neg__(x)

De nition at line 223 of le sundial.py.

10.172.2.7 def rpki.sundial.timedelta.__pos__(x)

De nition at line 224 of le sundial.py.

10.172.2.8 def rpki.sundial.timedelta.__radd__ (x, y)

De nition at line 225 of le sundial.py.

10.172.2.9 def rpki.sundial.timedelta.__rdiv__ (x, y)

De nition at line 226 of le sundial.py.

10.172.2.10 def rpki.sundial.timedelta.__r oordiv__ (x, y)

De nition at line 227 of le sundial.py.

10.172.2.11 def rpki.sundial.timedelta.__rmul__ (x, y)

De nition at line 228 of le sundial.py.

10.172.2.12 def rpki.sundial.timedelta.__rsub__ (x, y)

De nition at line 229 of le sundial.py.

10.172.2.13 def rpki.sundial.timedelta.__sub__ (x, y)

De nition at line 230 of le sundial.py.

10.172.2.14 def rpki.sundial.timedelta.convert_to_seconds (self)

Convert a timedelta interval to seconds.

De nition at line 209 of le sundial.py.

10.172.2.15 def rpki.sundial.timedelta.fromtimedelta (cls, x)

Convert a datetime.timedelta object into this subclass.

De nition at line 214 of le sundial.py.

10.172.2.16 def rpki.sundial.timedelta.parse (cls, arg)

Parse text into a timedelta object.

De nition at line 194 of le sundial.py.

10.172.3 Member Data Documentation

10.172.3.1 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.

De nition at line 185 of le sundial.py.

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

- sundial.py (2785)

10.173 rpki.up_down.base_elt Class Reference

Inherits object

Inherited by rpki.up_down.certi cate_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

10.173.1 Detailed Description

Generic PDU object.

Virtual class, just provides some default methods.

De nition at line 43 of le up_down.py.

10.173.2 Member Function Documentation

10.173.2.1 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

De nition at line 91 of le up_down.py.

10.173.2.2 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.certi cate_elt, rpki.up_down.class_elt, rpki.up_down.issue_pdu, and rpki.up_down.error_response_pdu.

De nition at line 59 of le up_down.py.

10.173.2.3 def rpki.up_down.base_elt.make_b64elt(self, elt, name, value = None)

Construct a sub-element with Base64 text content.

De nition at line 78 of le up_down.py.

10.173.2.4 def rpki.up_down.base_elt.make_elt(self, name, attrs)

Construct a element, copying over a set of attributes.

De nition at line 67 of le up_down.py.

10.173.2.5 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.

De nition at line 87 of le up_down.py.

10.173.2.6 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.certi cate_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.

De nition at line 50 of le up_down.py.

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

- up_down.py (2935)

10.174 rpki.up_down.certi cate_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

10.174.1 Detailed Description

Up-Down protocol representation of an issued certificate.

De nition at line 128 of le up_down.py.

10.174.2 Member Function Documentation

10.174.2.1 def rpki.up_down.certi cate_elt.endElement (self, stack, name, text)

Handle text content of a <certificate/> element.

Reimplemented from rpki.up_down.base_elt.

De nition at line 143 of le up_down.py.

10.174.2.2 def rpki.up_down.certi cate_elt.startElement (self, stack, name, attrs)

Handle attributes of <certificate/> element.

Reimplemented from rpki.up_down.base_elt.

De nition at line 133 of le up_down.py.

10.174.2.3 def rpki.up_down.certi cate_elt.toXML (self)

Generate a <certificate/> element.

De nition at line 151 of le up_down.py.

10.174.3 Member Data Documentation

10.174.3.1 rpki.up_down.certi cate_elt.cert

De nition at line 148 of le up_down.py.

10.174.3.2 rpki.up_down.certi cate_elt.cert_url

De nition at line 138 of le up_down.py.

10.174.3.3 rpki.up_down.certi cate_elt.req_resource_set_as

De nition at line 139 of le up_down.py.

10.174.3.4 rpki.up_down.certi cate_elt.req_resource_set_ipv4

De nition at line 140 of le up_down.py.

10.174.3.5 rpki.up_down.certi cate_elt.req_resource_set_ipv6

De nition at line 141 of le up_down.py.

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

- up_down.py (2935)

10.175 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

10.175.1 Detailed Description

Up-Down protocol representation of a resource class.

De nition at line 160 of le up_down.py.

10.175.2 Member Function Documentation

10.175.2.1 def rpki.up_down.class_elt.__init__(self)

Initialize class_elt.

De nition at line 167 of le up_down.py.

10.175.2.2 def rpki.up_down.class_elt.endElement(self, stack, name, text)

Handle <class/> elements and their children.

Reimplemented from rpki.up_down.base_elt.

De nition at line 191 of le up_down.py.

10.175.2.3 def rpki.up_down.class_elt.from_resource_bag(self, bag)

Set resources of this class element from a resource_bag.

De nition at line 222 of le up_down.py.

10.175.2.4 def rpki.up_down.class_elt.startElement(self, stack, name, attrs)

Handle <class/> elements and their children.

Reimplemented from rpki.up_down.base_elt.

De nition at line 172 of le up_down.py.

10.175.2.5 def rpki.up_down.class_elt.to_resource_bag(self)

Build a resource_bag from from this <class/> element.

De nition at line 213 of le up_down.py.

10.175.2.6 def rpki.up_down.class_elt.toXML (self)

Generate a <class/> element.

De nition at line 201 of le up_down.py.

10.175.3 Member Data Documentation

10.175.3.1 rpki.up_down.class_elt.cert_url

De nition at line 184 of le up_down.py.

10.175.3.2 rpki.up_down.class_elt.certs

De nition at line 170 of le up_down.py.

10.175.3.3 rpki.up_down.class_elt.class_name

De nition at line 183 of le up_down.py.

10.175.3.4 rpki.up_down.class_elt.issuer = None [static]

De nition at line 165 of le up_down.py.

10.175.3.5 rpki.up_down.class_elt.resource_set_as

De nition at line 186 of le up_down.py.

10.175.3.6 rpki.up_down.class_elt.resource_set_ipv4

De nition at line 187 of le up_down.py.

10.175.3.7 rpki.up_down.class_elt.resource_set_ipv6

De nition at line 188 of le up_down.py.

10.175.3.8 rpki.up_down.class_elt.resource_set_notafter

De nition at line 189 of le up_down.py.

10.175.3.9 rpki.up_down.class_elt.suggested_sia_head

De nition at line 185 of le up_down.py.

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

- up_down.py (2935)

10.176 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

10.176.1 Detailed Description

Syntax for Up-Down protocol "list_response" and "issue_response" PDUs.

De nition at line 284 of le up_down.py.

10.176.2 Member Function Documentation

10.176.2.1 def rpki.up_down.class_response_syntax.__init__(self)

Initialize class_response_syntax.

De nition at line 289 of le up_down.py.

10.176.2.2 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.

De nition at line 296 of le up_down.py.

10.176.2.3 def rpki.up_down.class_response_syntax.toXML(self)

Generate payload of "list_response" and "issue_response" PDUs.

De nition at line 306 of le up_down.py.

10.176.3 Member Data Documentation

10.176.3.1 rpki.up_down.class_response_syntax.classes

De nition at line 294 of le up_down.py.

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

- up_down.py (2935)

10.177 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

10.177.1 Detailed Description

Class to hold a CMS-signed up-down PDU.

De nition at line 682 of le up_down.py.

10.177.2 Member Data Documentation

10.177.2.1 string rpki.up_down.cms_msg.encoding = "UTF-8" [static]

De nition at line 687 of le up_down.py.

10.177.2.2 rpki.up_down.cms_msg.saxify = sax_handler.saxify [static]

Reimplemented in rootd.cms_msg.

De nition at line 689 of le up_down.py.

10.177.2.3 rpki.up_down.cms_msg.schema = rpki.relaxng.up_down [static]

De nition at line 688 of le up_down.py.

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

- up_down.py (2935)

10.178 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

10.178.1 Detailed Description

Up-Down protocol "error_response" PDU.

Definition at line 502 of file up_down.py.

10.178.2 Member Function Documentation

10.178.2.1 def rpki.up_down.error_response_pdu.__init__(self, exception=None)

Initialize an error_response PDU from an exception object.

Definition at line 521 of file up_down.py.

10.178.2.2 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 561 of file up_down.py.

10.178.2.3 def rpki.up_down.error_response_pdu.endElement(self, stack, name, text)

Handle "error_response" PDU.

Reimplemented from rpki.up_down.base_elt.

De nition at line 530 of le up_down.py.

10.178.2.4 def rpki.up_down.error_response_pdu.toXML(self)

Generate payload of "error_response" PDU.

De nition at line 546 of le up_down.py.

10.178.3 Member Data Documentation

10.178.3.1 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" }
```

De nition at line 507 of le up_down.py.

10.178.3.2 rpki.up_down.error_response_pdu.description

De nition at line 528 of le up_down.py.

10.178.3.3 dictionary rpki.up_down.error_response_pdu.exceptions [static]

Initial value:

```
{
    rpki.exceptions.NoActiveCA : 1202 }
```

De nition at line 518 of le up_down.py.

10.178.3.4 rpki.up_down.error_response_pdu.status

De nition at line 527 of le up_down.py.

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

- up_down.py (2935)

10.179 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

10.179.1 Detailed Description

Up-Down protocol "issue" PDU.

De nition at line 316 of le up_down.py.

10.179.2 Member Function Documentation

10.179.2.1 def rpki.up_down.issue_pdu.endElement(self, stack, name, text)

Handle "issue" PDU.

Reimplemented from rpki.up_down.base_elt

De nition at line 331 of le up_down.py.

10.179.2.2 def rpki.up_down.issue_pdu.query(cls, parent, ca, ca_detail, callback, errback)

Send an "issue" request to parent associated with ca.

De nition at line 417 of le up_down.py.

10.179.2.3 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

De nition at line 348 of le up_down.py.

10.179.2.4 def rpki.up_down.issue_pdu.startElement(self, stack, name, attrs)

Handle "issue" PDU.

Reimplemented from rpki.up_down.base_elt

De nition at line 321 of le up_down.py.

10.179.2.5 def rpki.up_down.issue_pdu.toXML (self)

Generate payload of "issue" PDU.

De nition at line 339 of le up_down.py.

10.179.3 Member Data Documentation

10.179.3.1 rpki.up_down.issue_pdu.class_name

De nition at line 326 of le up_down.py.

10.179.3.2 rpki.up_down.issue_pdu.pkcs10

De nition at line 336 of le up_down.py.

10.179.3.3 rpki.up_down.issue_pdu.req_resource_set_as

De nition at line 327 of le up_down.py.

10.179.3.4 rpki.up_down.issue_pdu.req_resource_set_ipv4

De nition at line 328 of le up_down.py.

10.179.3.5 rpki.up_down.issue_pdu.req_resource_set_ipv6

De nition at line 329 of le up_down.py.

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

- up_down.py (2935)

10.180 rpki.up_down.issue_response_pdu Class Reference

Inherits rpki::up_down::class_response_syntax.

Public Member Functions

- def check_response

10.180.1 Detailed Description

Up-Down protocol "issue_response" PDU.

De nition at line 429 of le up_down.py.

10.180.2 Member Function Documentation

10.180.2.1 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.

De nition at line 434 of le up_down.py.

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

- up_down.py (2935)

10.181 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

10.181.1 Detailed Description

Up-Down protocol "list" PDU.

De nition at line 231 of le up_down.py.

10.181.2 Member Function Documentation

10.181.2.1 def rpki.up_down.list_pdu.query (cls, parent, cb, eb)

Send a "list" query to parent.

De nition at line 273 of le up_down.py.

10.181.2.2 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.

De nition at line 240 of le up_down.py.

10.181.2.3 def rpki.up_down.list_pdu.toXML (self)

Generate (empty) payload of "list" PDU.

De nition at line 236 of le up_down.py.

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

- up_down.py (2935)

10.182 rpki.up_down.list_response_pdu Class Reference

Inherits rpki::up_down::class_response_syntax.

10.182.1 Detailed Description

Up-Down protocol "list_response" PDU.

De nition at line 310 of le up_down.py.

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

- up_down.py (2935)

10.183 rpki.up_down.message_pdu Class Reference

Inheritsrpki::up_down::base_elt

Inherited byrootd.message_pdu

Public Member Functions

- def __str__
- def log_query
- def make_query
- def serve_error
- def serve_top_level
- def startElement
- def toXML

Public Attributes

- payload
- recipient
- sender
- type
- version

Static Public Attributes

- dictionaryname2type
- tuple type2name= dict((v, k) for k, v in name2type.items())
- int version= 1

10.183.1 Detailed Description

Up-Down protocol message wrapper PDU.

De nition at line 568 of le up_down.py.

10.183.2 Member Function Documentation

10.183.2.1 def rpki.up_down.message_pdu.__str__(self)

Convert a message PDU to a string.

De nition at line 610 of le up_down.py.

10.183.2.2 def rpki.up_down.message_pdu.log_query(self, child)

Log query we're handling. Separate method so rootd can override.

Reimplemented in rootd.message_pdu

De nition at line 639 of le up_down.py.

10.183.2.3 def rpki.up_down.message_pdu.make_query(cls, payload, sender, recipient)

Construct one message PDU.

De nition at line 657 of le up_down.py.

10.183.2.4 def rpki.up_down.message_pdu.serve_error(self, exception)

Generate an error_response message PDU.

De nition at line 645 of le up_down.py.

10.183.2.5 def rpki.up_down.message_pdu.serve_top_level(self, child, callback)

Serve one message request PDU.

De nition at line 614 of le up_down.py.

10.183.2.6 def rpki.up_down.message_pdu.startElement(self, stack, name, attrs)

Handle message PDU.

Payload of the <message/> element varies depending on the "type" attribute, so after some basic checks we have to instantiate the right class object to handle whatever kind of PDU this is.

Reimplemented from rpki.up_down.base_elt

De nition at line 594 of le up_down.py.

10.183.2.7 def rpki.up_down.message_pdu.toXML(self)

Generate payload of message PDU.

De nition at line 586 of le up_down.py.

10.183.3 Member Data Documentation

10.183.3.1 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

De nition at line 575 of le up_down.py.

10.183.3.2 rpki.up_down.message_pdu.payload

De nition at line 607 of le up_down.py.

10.183.3.3 rpki.up_down.message_pdu.recipient

De nition at line 605 of le up_down.py.

10.183.3.4 rpki.up_down.message_pdu.sender

De nition at line 604 of le up_down.py.

10.183.3.5 rpki.up_down.message_pdu.type

De nition at line 606 of le up_down.py.

10.183.3.6 tuple rpki.up_down.message_pdu.type2name = dict((v, k) for k, v in name2type.items()) [static]

Reimplemented in rootd.message_pdu.

De nition at line 584 of le up_down.py.

10.183.3.7 rpki.up_down.message_pdu.version

De nition at line 603 of le up_down.py.

10.183.3.8 int rpki.up_down.message_pdu.version = 1 [static]

De nition at line 573 of le up_down.py.

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

- up_down.py (2935)

10.184 rpki.up_down.multi_uri Class Reference

Inherits list.

Public Member Functions

- def __init__
- def __str__
- def rsync

10.184.1 Detailed Description

Container for a set of URIs.

De nition at line 95 of le up_down.py.

10.184.2 Member Function Documentation

10.184.2.1 def rpki.up_down.multi_uri.__init__ (self, ini)

Initialize a set of URIs, which includes basic some syntax checking.

De nition at line 100 of le up_down.py.

10.184.2.2 def rpki.up_down.multi_uri.__str__ (self)

Convert a multi_uri back to a string representation.

De nition at line 115 of le up_down.py.

10.184.2.3 def rpki.up_down.multi_uri.rsync (self)

Find first rsync://... URI in self.

De nition at line 119 of le up_down.py.

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

- up_down.py (2935)

10.185 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

10.185.1 Detailed Description

Up-Down protocol "revoke" PDU.

De nition at line 456 of le up_down.py.

10.185.2 Member Function Documentation

10.185.2.1 def rpki.up_down.revoke_pdu.get_SKI(self)

Convert g(SKI) encoding from PDU back to raw SKI.

De nition at line 461 of le up_down.py.

10.185.2.2 def rpki.up_down.revoke_pdu.query(cls, ca, gski, cb, eb)

Send a "revoke" request for certificate(s) named by gski to parent associated with ca.

Definition at line 485 of file up_down.py.

10.185.2.3 def rpki.up_down.revoke_pdu.serve_pdus(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 465 of file up_down.py.

10.185.3 Member Data Documentation

10.185.3.1 rpki.up_down.revoke_pdu.class_name

Reimplemented from rpki.up_down.revoke_syntax.

Definition at line 491 of file up_down.py.

10.185.3.2 rpki.up_down.revoke_pdu.ski

Reimplemented from rpki.up_down.revoke_syntax.

Definition at line 492 of file up_down.py.

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

- up_down.py (2935)

10.186 rpki.up_down.revoke_response_pdu Class Reference

Inherits rpki::up_down::revoke_syntax.

10.186.1 Detailed Description

Up-Down protocol "revoke_response" PDU.

De nition at line 495 of le up_down.py.

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

- up_down.py (2935)

10.187 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

10.187.1 Detailed Description

Syntax for Up-Down protocol "revoke" and "revoke_response" PDUs.

De nition at line 442 of le up_down.py.

10.187.2 Member Function Documentation

10.187.2.1 def rpki.up_down.revoke_syntax.startElement(self, stack, name, attrs)

Handle "revoke" PDU.

Reimplemented from rpki.up_down.base_elt.

De nition at line 447 of le up_down.py.

10.187.2.2 def rpki.up_down.revoke_syntax.toXML (self)

Generate payload of "revoke" PDU.

De nition at line 452 of le up_down.py.

10.187.3 Member Data Documentation

10.187.3.1 rpki.up_down.revoke_syntax.class_name

Reimplemented in rpki.up_down.revoke_pdu

De nition at line 449 of le up_down.py.

10.187.3.2 rpki.up_down.revoke_syntax.ski

Reimplemented in rpki.up_down.revoke_pdu

De nition at line 450 of le up_down.py.

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

- up_down.py (2935)

10.188 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"

10.188.1 Detailed Description

SAX handler for Up-Down protocol.

De nition at line 673 of le up_down.py.

10.188.2 Member Data Documentation

10.188.2.1 string rpki.up_down.sax_handler.name = "message" [static]

Definition at line 679 of file up_down.py.

10.188.2.2 rpki.up_down.sax_handler.pdu = message_pdu [static]

Reimplemented in rootd.sax_handler.

Definition at line 678 of file up_down.py.

10.188.2.3 string rpki.up_down.sax_handler.version = "1" [static]

Definition at line 680 of file up_down.py.

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

- up_down.py (2935)

10.189 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 = POW.pkix.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 = POW.pemConverter("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.

10.189.1 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.

De nition at line 702 of le x509.py.

10.189.2 Member Function Documentation

10.189.2.1 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.

De nition at line 853 of le x509.py.

10.189.2.2 def rpki.x509.CMS_object.get_contents(self)

Get the inner content of this CMS_object.

De nition at line 764 of le x509.py.

10.189.2.3 def rpki.x509.CMS_object.get_DER(self)

Get the DER value of this CMS_object.

Reimplemented from rpki.x509.DER_object.

De nition at line 743 of le x509.py.

10.189.2.4 def rpki.x509.CMS_object.get_POW(self)

Get the POW value of this CMS_object.

De nition at line 755 of le x509.py.

10.189.2.5 def rpki.x509.CMS_object.set_content(self, content)

Set the (inner) content of this CMS_object, clearing the wrapper.

Definition at line 772 of file x509.py.

10.189.2.6 def rpki.x509.CMS_object.sign(self, keypair, certs, crls = None, no_certs = False)

Sign and wrap inner content.

Definition at line 881 of file x509.py.

10.189.2.7 def rpki.x509.CMS_object.verify(self, ta)

Verify CMS wrapper and store inner content.

Definition at line 779 of file x509.py.

10.189.3 Member Data Documentation

10.189.3.1 rpki.x509.CMS_object.content

Reimplemented in rpki.x509.DER_CMS_object, and rpki.x509.XML_CMS_object.

Definition at line 777 of file x509.py.

10.189.3.2 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 728 of file x509.py.

10.189.3.3 rpki.x509.CMS_object.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

De nition at line 751 of le x509.py.

10.189.3.4 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.

De nition at line 723 of le x509.py.

10.189.3.5 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.

De nition at line 717 of le x509.py.

10.189.3.6 tuple rpki.x509.CMS_object.formats = ("DER", "POW") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

De nition at line 715 of le x509.py.

10.189.3.7 tuple rpki.x509.CMS_object.other_clear = ("content",) [static]

Other attributes that self.clear() should whack.

Reimplemented from rpki.x509.DER_object.

De nition at line 716 of le x509.py.

10.189.3.8 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.

De nition at line 718 of le x509.py.

10.189.3.9 rpki.x509.CMS_object.POW

De nition at line 761 of le x509.py.

10.189.3.10 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.

De nition at line 741 of le x509.py.

10.189.3.11 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 uncondtionally mandatory in such cases.

De nition at line 735 of le x509.py.

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

- x509.py (2928)

10.190 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

10.190.1 Detailed Description

Class to hold a Certificate Revocation List.

Definition at line 1107 of file x509.py.

10.190.2 Member Function Documentation

10.190.2.1 def rpki.x509.CRL.generate(cls, keypair, issuer, serial, thisUpdate, nextUpdate, revokedCertificates, version = 1, digestType = "sha256WithRSAEncryption")

Generate a new CRL.

Definition at line 1163 of file x509.py.

10.190.2.2 def rpki.x509.CRL.get_DER (self)

Get the DER value of this CRL.

Reimplemented from rpki.x509.DER_object.

De nition at line 1115 of le x509.py.

10.190.2.3 def rpki.x509.CRL.get_POW (self)

Get the POW value of this CRL.

De nition at line 1130 of le x509.py.

10.190.2.4 def rpki.x509.CRL.get_POWpkix (self)

Get the POW.pkix value of this CRL.

De nition at line 1139 of le x509.py.

10.190.2.5 def rpki.x509.CRL.getIssuer (self)

Get issuer value of this CRL.

De nition at line 1158 of le x509.py.

10.190.2.6 def rpki.x509.CRL.getNextUpdate (self)

Get nextUpdate value from this CRL.

De nition at line 1154 of le x509.py.

10.190.2.7 def rpki.x509.CRL.getThisUpdate (self)

Get thisUpdate value from this CRL.

De nition at line 1150 of le x509.py.

10.190.3 Member Data Documentation

10.190.3.1 rpki.x509.CRL.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

De nition at line 1123 of le x509.py.

10.190.3.2 tuple rpki.x509.CRL.formats = ("DER", "POW", "POWpkix") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

De nition at line 1112 of le x509.py.

10.190.3.3 tuple rpki.x509.CRL.pem_converter = PEM_converter("X509 CRL") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

De nition at line 1113 of le x509.py.

10.190.3.4 rpki.x509.CRL.POW

De nition at line 1136 of le x509.py.

10.190.3.5 rpki.x509.CRL.POWpkix

De nition at line 1147 of le x509.py.

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

- x509.py (2928)

10.191 rpki.x509.DeadDrop Class Reference

Inheritsobject.

Public Member Functions

- def __init__
- def dump

Public Attributes

- maildir
- pid

10.191.1 Detailed Description

Dead-drop utility for storing copies of CMS messages for debugging or audit. At the moment this uses Maildir mailbox format, as it has approximately the right properties and a number of useful tools for manipulating it already exist.

De nition at line 1002 of le x509.py.

10.191.2 Member Function Documentation

10.191.2.1 def rpki.x509.DeadDrop.__init__(self, name)

De nition at line 1010 of le x509.py.

10.191.2.2 def rpki.x509.DeadDrop.dump (self, obj)

De nition at line 1014 of le x509.py.

10.191.3 Member Data Documentation

10.191.3.1 rpki.x509.DeadDrop.maildir

De nition at line 1011 of le x509.py.

10.191.3.2 rpki.x509.DeadDrop.pid

De nition at line 1012 of le x509.py.

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

- x509.py (2928)

10.192 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

10.192.1 Detailed Description

Class to hold CMS objects with DER-based content.

De nition at line 917 of le x509.py.

10.192.2 Member Function Documentation

10.192.2.1 def rpki.x509.DER_CMS_object.decode(self, der)

Decode DER and set inner content.

Definition at line 926 of file x509.py.

10.192.2.2 def rpki.x509.DER_CMS_object.encode(self)

Encode inner content for signing.

Definition at line 922 of file x509.py.

10.192.3 Member Data Documentation

10.192.3.1 rpki.x509.DER_CMS_object.content

Reimplemented from rpki.x509.CMS_object

Definition at line 932 of file x509.py.

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

- x509.py (2928)

10.193 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

10.193.1 Detailed Description

Virtual class to hold a generic DER object.

De nition at line 105 of le x509.py.

10.193.2 Member Function Documentation

10.193.2.1 def rpki.x509.DER_object.__cmp__(self, other)

Compare two DER-encoded objects.

Definition at line 200 of file x509.py.

10.193.2.2 def rpki.x509.DER_object.__init__(self, kw)

Initialize a DER_object.

Definition at line 138 of file x509.py.

10.193.2.3 def rpki.x509.DER_object.clear(self)

Make this object empty.

Definition at line 131 of file x509.py.

10.193.2.4 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 308 of file x509.py.

10.193.2.5 def rpki.x509.DER_object.empty(self)

Test whether this object is empty.

Definition at line 122 of file x509.py.

10.193.2.6 def rpki.x509.DER_object.from_sql(cls, x)

Convert from SQL storage format.

De nition at line 300 of le x509.py.

10.193.2.7 def rpki.x509.DER_object.gAKI(self)

Calculate g(AKI) for this object. Only work for subclasses that implement get_AKI().

De nition at line 236 of le x509.py.

10.193.2.8 def rpki.x509.DER_object.get_3779resources(self)

Get RFC 3779 resources as rpki.resource_set objects. Only works for subclasses that support getExtensions().

De nition at line 287 of le x509.py.

10.193.2.9 def rpki.x509.DER_object.get_AIA(self)

Get the SIA extension from this object. Only works for subclasses that support getExtension().

De nition at line 265 of le x509.py.

10.193.2.10 def rpki.x509.DER_object.get_AKI(self)

Get the AKI extension from this object. Only works for subclasses that support getExtension().

De nition at line 243 of le x509.py.

10.193.2.11 def rpki.x509.DER_object.get_Base64(self)

Get the Base64 encoding of the DER value of this object.

Definition at line 192 of file x509.py.

10.193.2.12 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 272 of file x509.py.

10.193.2.13 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 181 of file x509.py.

10.193.2.14 def rpki.x509.DER_object.get_PEM(self)

Get the PEM representation of this object.

Definition at line 196 of file x509.py.

10.193.2.15 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 258 of file x509.py.

10.193.2.16 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.

De nition at line 251 of le x509.py.

10.193.2.17 def rpki.x509.DER_object.gSKI(self)

Calculate g(SKI) for this object. Only work for subclasses that implement get_SKI().

De nition at line 221 of le x509.py.

10.193.2.18 def rpki.x509.DER_object.hAKI(self)

Return hexadecimal string representation of AKI for this object. Only work for subclasses that implement get_AKI().

De nition at line 228 of le x509.py.

10.193.2.19 def rpki.x509.DER_object.hSKI(self)

Return hexadecimal string representation of SKI for this object. Only work for subclasses that implement get_SKI().

De nition at line 213 of le x509.py.

10.193.2.20 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.

De nition at line 279 of le x509.py.

10.193.2.21 def rpki.x509.DER_object.sets(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.

De nition at line 146 of le x509.py.

10.193.2.22 def rpki.x509.DER_object.to_sql(self)

Convert to SQL storage format.

De nition at line 304 of le x509.py.

10.193.3 Member Data Documentation

10.193.3.1 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.

De nition at line 164 of le x509.py.

10.193.3.2 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.

De nition at line 111 of le x509.py.

10.193.3.3 tuple rpki.x509.DER_object.other_clear = () [static]

Other attributes that self.clear() should whack.

Reimplemented in rpki.x509.CMS_object.

De nition at line 117 of le x509.py.

10.193.3.4 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.

De nition at line 114 of le x509.py.

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

- x509.py (2928)

10.194 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

10.194.1 Detailed Description

Convert between DER and PEM encodings for various kinds of ASN.1 data.

De nition at line 62 of le x509.py.

10.194.2 Member Function Documentation

10.194.2.1 def rpki.x509.PEM_converter.__init__ (self, kind)

Initialize PEM_converter.

De nition at line 67 of le x509.py.

10.194.2.2 def rpki.x509.PEM_converter.looks_like_PEM (self, text)

Guess whether text looks like a PEM encoding.

De nition at line 74 of le x509.py.

10.194.2.3 def rpki.x509.PEM_converter.to_DER (self, pem)

Convert from PEM to DER.

De nition at line 81 of le x509.py.

10.194.2.4 def rpki.x509.PEM_converter.to_PEM (self, der)

Convert from DER to PEM.

De nition at line 94 of le x509.py.

10.194.3 Member Data Documentation

10.194.3.1 rpki.x509.PEM_converter.b

De nition at line 71 of le x509.py.

10.194.3.2 rpki.x509.PEM_converter.e

De nition at line 72 of le x509.py.

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

- x509.py (2928)

10.195 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.

10.195.1 Detailed Description

Class to hold a PKCS #10 request.

De nition at line 501 of le x509.py.

10.195.2 Member Function Documentation

10.195.2.1 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 536 of file x509.py.

10.195.2.2 def rpki.x509.PKCS10.create(cls, keypair, exts = None)

Create a new request for a given keypair, including given extensions.

Definition at line 596 of file x509.py.

10.195.2.3 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 583 of file x509.py.

10.195.2.4 def rpki.x509.PKCS10.get_DER(self)

Get the DER value of this certification request.

Reimplemented from rpki.x509.DER_object.

Definition at line 509 of file x509.py.

10.195.2.5 def rpki.x509.PKCS10.get_POWpkix(self)

Get the POW.pkix value of this certification request.

Definition at line 521 of file x509.py.

10.195.2.6 def rpki.x509.PKCS10.getPublicKey(self)

Extract the public key from this certification request.

De nition at line 532 of le x509.py.

10.195.3 Member Data Documentation

10.195.3.1 rpki.x509.PKCS10.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

De nition at line 517 of le x509.py.

10.195.3.2 tuple rpki.x509.PKCS10.formats = ("DER", "POWpkix") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

De nition at line 506 of le x509.py.

10.195.3.3 tuple rpki.x509.PKCS10.pem_converter = PEM_converter("CERTIFICATE REQUEST") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

De nition at line 507 of le x509.py.

10.195.3.4 rpki.x509.PKCS10.POWpkix

De nition at line 529 of le x509.py.

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

- x509.py (2928)

10.196 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

10.196.1 Detailed Description

Class to hold a signed ROA.

Definition at line 974 of file x509.py.

10.196.2 Member Function Documentation

10.196.2.1 def rpki.x509.ROA.build (cls, asn, ipv4, ipv6, keypair, certs, version = 0)

Build a ROA.

Definition at line 984 of file x509.py.

10.196.3 Member Data Documentation

10.196.3.1 rpki.x509.ROA.content_class = rpki.roa.RouteOriginAttestation [static]

Definition at line 980 of file x509.py.

10.196.3.2 tuple rpki.x509.ROA.econtent_oid = POWify_OID("id-ct-routeOriginAttestation") [static]

Reimplemented from rpki.x509.CMS_object

De nition at line 981 of le x509.py.

10.196.3.3 tuple rpki.x509.ROA.pem_converter = PEM_converter("ROUTE ORIGIN ATTESTATION") [static]

PEM converter for this object.

Reimplemented from rpki.x509.CMS_object.

De nition at line 979 of le x509.py.

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

- x509.py (2928)

10.197 rpki.x509.RSA Class Reference

Inherits rpki::x509::DER_object

Public Member Functions

- def generate
- def get_DER
- def get_POW
- def get_public_DER
- def get_RSApublic
- def get_SKI

Public Attributes

- DER

  DER value of this object.

- POW

Static Public Attributes

- tuple formats = ("DER", "POW")
  Formats supported in this object
- tuple pem_converter = PEM_converter("RSA PRIVATE KEY")
  PEM converter for this object.

10.197.1 Detailed Description

Class to hold an RSA key pair.

Definition at line 610 of file x509.py.

10.197.2 Member Function Documentation

10.197.2.1 def rpki.x509.RSA.generate(self, keylength = 2048)

Generate a new keypair.

Definition at line 640 of file x509.py.

10.197.2.2 def rpki.x509.RSA.get_DER(self)

Get the DER value of this keypair.

Reimplemented from rpki.x509.DER_object.

Definition at line 618 of file x509.py.

10.197.2.3 def rpki.x509.RSA.get_POW(self)

Get the POW value of this keypair.

Definition at line 630 of file x509.py.

10.197.2.4 def rpki.x509.RSA.get_public_DER(self)

Get the DER encoding of the public key from this keypair.

De nition at line 647 of le x509.py.

10.197.2.5 def rpki.x509.RSA.get_RSApublic(self)

Convert the public key of this keypair into a RSApublic object.

De nition at line 655 of le x509.py.

10.197.2.6 def rpki.x509.RSA.get_SKI(self)

Calculate the SKI of this keypair.

Reimplemented from rpki.x509.DER_object.

De nition at line 651 of le x509.py.

10.197.3 Member Data Documentation

10.197.3.1 rpki.x509.RSA.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

De nition at line 626 of le x509.py.

10.197.3.2 tuple rpki.x509.RSA.formats = ("DER", "POW") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

De nition at line 615 of le x509.py.

10.197.3.3 tuple rpki.x509.RSA.pem_converter = PEM_converter("RSA PRIVATE KEY") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

De nition at line 616 of le x509.py.

10.197.3.4 rpki.x509.RSA.POW

De nition at line 636 of le x509.py.

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

- x509.py (2928)

10.198 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.

10.198.1 Detailed Description

Class to hold an RSA public key.

Definition at line 659 of file x509.py.

10.198.2 Member Function Documentation

10.198.2.1 def rpki.x509.RSApublic.get_DER(self)

Get the DER value of this public key.

Reimplemented from rpki.x509.DER_object.

Definition at line 667 of file x509.py.

10.198.2.2 def rpki.x509.RSApublic.get_POW(self)

Get the POW value of this public key.

Definition at line 679 of file x509.py.

10.198.2.3 def rpki.x509.RSApublic.get_SKI(self)

Calculate the SKI of this public key.

Reimplemented from rpki.x509.DER_object.

Definition at line 688 of file x509.py.

10.198.3 Member Data Documentation

10.198.3.1 rpki.x509.RSApublic.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

De nition at line 675 of le x509.py.

10.198.3.2 tuple rpki.x509.RSApublic.formats = ("DER", "POW") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

De nition at line 664 of le x509.py.

10.198.3.3 tuple rpki.x509.RSApublic.pem_converter = PEM_converter("RSA PUBLIC KEY") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

De nition at line 665 of le x509.py.

10.198.3.4 rpki.x509.RSApublic.POW

De nition at line 685 of le x509.py.

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

- x509.py (2928)

10.199 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

10.199.1 Detailed Description

Class to hold a signed manifest.

Definition at line 934 of file x509.py.

10.199.2 Member Function Documentation

10.199.2.1 def rpki.x509.SignedManifest.build(cls, serial, thisUpdate, nextUpdate, names_and_objs, keypair, certs, version = 0)

Build a signed manifest.

Definition at line 952 of file x509.py.

10.199.2.2 def rpki.x509.SignedManifest.getNextUpdate(self)

Get nextUpdate value from this manifest.

Definition at line 947 of file x509.py.

10.199.2.3 def rpki.x509.SignedManifest.getThisUpdate(self)

Get thisUpdate value from this manifest.

Definition at line 943 of file x509.py.

10.199.3 Member Data Documentation

10.199.3.1 rpki.x509.SignedManifest.content_class = rpki.manifest.Manifest [static]

De nition at line 940 of le x509.py.

10.199.3.2 tuple rpki.x509.SignedManifest.econtent_oid = POWify_OID("id-ct-rpkiManifest") [static]

Reimplemented from rpki.x509.CMS_object.

De nition at line 941 of le x509.py.

10.199.3.3 tuple rpki.x509.SignedManifest.pem_converter = PEM_converter("RPKI MANIFEST") [static]

PEM converter for this object.

Reimplemented from rpki.x509.CMS_object.

De nition at line 939 of le x509.py.

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

- x509.py (2928)

10.200 rpki.x509.X509 Class Reference

Inherits rpki::x509::DER_object

Public Member Functions

- def cross_certify
- def expired
- def get_DER
- def get_POW
- def get_POWpkix
- def getIssuer
- def getNotAfter

- def getNotBefore
- def getPublicKey
- def getSerial
- def getSubject
- def issue
- def normalize_chain

Public Attributes

- DER
  DER value of this object
- POW
- POWpkix

Static Public Attributes

- tuple formats = ("DER", "POW", "POWpkix")
  Formats supported in this object
- tuple pem_converter = PEM_converter("CERTIFICATE")
  PEM converter for this object

10.200.1 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.

De nition at line 327 of le x509.py.

10.200.2 Member Function Documentation

10.200.2.1 def rpki.x509.X509.cross_certify(self, keypair, source_cert, serial, notAfter, now = None, pathLenConstraint = 0)

Issue a certificate with values taking from an existing certificate. This is used to construct some kinds oF BPKI certificates.

De nition at line 459 of le x509.py.

10.200.2.2 def rpki.x509.X509.expired(self)

Test whether this certificate has expired.

De nition at line 400 of le x509.py.

10.200.2.3 def rpki.x509.X509.get_DER(self)

Get the DER value of this certificate.

Reimplemented from rpki.x509.DER_object.

De nition at line 341 of le x509.py.

10.200.2.4 def rpki.x509.X509.get_POW(self)

Get the POW value of this certificate.

De nition at line 356 of le x509.py.

10.200.2.5 def rpki.x509.X509.get_POWpkix(self)

Get the POW.pkix value of this certificate.

De nition at line 365 of le x509.py.

10.200.2.6 def rpki.x509.X509.getIssuer(self)

Get the issuer of this certificate.

De nition at line 376 of le x509.py.

10.200.2.7 def rpki.x509.X509.getNotAfter(self)

Get the expiration time of this certificate.

De nition at line 388 of le x509.py.

10.200.2.8 def rpki.x509.X509.getNotBefore(self)

Get the inception time of this certificate.

De nition at line 384 of le x509.py.

10.200.2.9 def rpki.x509.X509.getPublicKey(self)

Extract the public key from this certificate.

De nition at line 396 of le x509.py.

10.200.2.10 def rpki.x509.X509.getSerial(self)

Get the serial number of this certificate.

De nition at line 392 of le x509.py.

10.200.2.11 def rpki.x509.X509.getSubject(self)

Get the subject of this certificate.

De nition at line 380 of le x509.py.

10.200.2.12 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 404 of file x509.py.

10.200.2.13 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 488 of file x509.py.

10.200.3 Member Data Documentation

10.200.3.1 rpki.x509.X509.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 349 of file x509.py.

10.200.3.2 tuple rpki.x509.X509.formats = ("DER", "POW", "POWpkix") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 338 of file x509.py.

10.200.3.3 tuple rpki.x509.X509.pem_converter = PEM_converter("CERTIFICATE") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

De nition at line 339 of le x509.py.

10.200.3.4 rpki.x509.X509.POW

De nition at line 362 of le x509.py.

10.200.3.5 rpki.x509.X509.POWpkix

De nition at line 373 of le x509.py.

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

- x509.py (2928)

10.201 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
  If set, we write all inbound XML-CMS PDUs to disk, for debugging.
- dump_outbound_cms = None
  If set, we write all outbound XML-CMS PDUs to disk, for debugging.
- tuple econtent_oid = POWify_OID("id-ct-xml")

10.201.1 Detailed Description

Class to hold CMS-wrapped XML protocol data.

De nition at line 1025 of le x509.py.

10.201.2 Member Function Documentation

10.201.2.1 def rpki.x509.XML_CMS_object.decode(self, xml)

Decode XML and set inner content.

De nition at line 1048 of le x509.py.

10.201.2.2 def rpki.x509.XML_CMS_object.dump_to_disk(self, pre x)

Write DER of current message to disk, for debugging.

De nition at line 1066 of le x509.py.

10.201.2.3 def rpki.x509.XML_CMS_object.encode(self)

Encode inner content for signing.

De nition at line 1044 of le x509.py.

10.201.2.4 def rpki.x509.XML_CMS_object.pretty_print_content (self)

Pretty print XML content of this message.

Definition at line 1052 of file x509.py.

10.201.2.5 def rpki.x509.XML_CMS_object.schema_check (self)

Handle XML RelaxNG schema check.

Definition at line 1056 of file x509.py.

10.201.2.6 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 1092 of file x509.py.

10.201.2.7 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 1075 of file x509.py.

10.201.3 Member Data Documentation

10.201.3.1 rpki.x509.XML_CMS_object.content

Reimplemented from rpki.x509.CMS_object.

Definition at line 1050 of file x509.py.

10.201.3.2 rpki::x509.XML_CMS_object::dump_inbound_cms = None [static]

If set, we write all inbound XML-CMS PDUs to disk, for debugging. If set, value should be a DeadDrop object.

De nition at line 1042 of le x509.py.

10.201.3.3 rpki::x509.XML_CMS_object::dump_outbound_cms = None [static]

If set, we write all outbound XML-CMS PDUs to disk, for debugging. If set, value should be a DeadDrop object.

De nition at line 1036 of le x509.py.

10.201.3.4 tuple rpki.x509.XML_CMS_object.econtent_oid = POWify_OID("id-ct-xml") [static]

Reimplemented from rpki.x509.CMS_object.

De nition at line 1030 of le x509.py.

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

- x509.py (2928)

10.202 rpki.xml_utils.base_elt Class Reference

Inherits object.

Inherited by rpki.left_right.list_resources_elt, rpki.left_right.list_roa_requests_elt, rpki.publication.publication_object_elt, rpki.xml_utils.data_elt, and rpki.xml_utils.text_elt.

Public Member Functions

- def __str__
- def endElement
- def make_b64elt
- def make_elt

- def make_pdu
- def read_attrs
- def startElement
- def toXML

Static Public Attributes

- tuple attributes = ()

  XML attributes for this element.

- tuple booleans = ()

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

- tuple elements = ()

  XML elements contained by this element.

10.202.1 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.

De nition at line 126 of le xml_utils.py.

10.202.2 Member Function Documentation

10.202.2.1 def rpki.xml_utils.base_elt.__str__(self)

Convert a base_elt object to string format.

Reimplemented in rpki.publication.report_error_elt.

De nition at line 201 of le xml_utils.py.

10.202.2.2 def rpki.xml_utils.base_elt.endElement(self, stack, name, text)

Default endElement() handler: just pop the stack.

Reimplemented in rpki.left_right.child_elt, rpki.publication.client_elt, rpki.publication.publication_object_elt, rpki.xml_utils.text_elt, and rpki.xml_utils.data_elt.

De nition at line 153 of le xml_utils.py.

10.202.2.3 def rpki.xml_utils.base_elt.make_b64elts(self, elt, name, value = None)

Constructor for Base64-encoded subelement.

De nition at line 192 of le xml_utils.py.

10.202.2.4 def rpki.xml_utils.base_elt.make_elts(self)

XML element constructor.

De nition at line 178 of le xml_utils.py.

10.202.2.5 def rpki.xml_utils.base_elt.make_pdu(cls, kargs)

Generic PDU constructor.

De nition at line 208 of le xml_utils.py.

10.202.2.6 def rpki.xml_utils.base_elt.read_attrs(self, attrs)

Template-driven attribute reader.

De nition at line 166 of le xml_utils.py.

10.202.2.7 def rpki.xml_utils.base_elt.startElement(self, stack, name, attrs)

Default startElement() handler: just process attributes.

Reimplemented in rpki.left_right.list_resources_elt, rpki.left_right.list_roa_requests_elt, and rpki.publication.con g_elt.

De nition at line 145 of le xml_utils.py.

10.202.2.8 def rpki.xml_utils.base_elt.toXML (self)

Default toXML() element generator.

Reimplemented in rpki.left_right.list_resources_elt, rpki.publication.publication_object_elt, rpki.xml_utils.text_elt, and rpki.xml_utils.data_elt.

De nition at line 160 of le xml_utils.py.

10.202.3 Member Data Documentation

10.202.3.1 rpki::xml_utils.base_elt::attributes = () [static]

XML attributes for this element.

Reimplemented in rpki.left_right.self_elt, rpki.left_right.bsc_elt, rpki.left_right.repository_elt, rpki.left_right.parent_elt, rpki.left_right.child_elt, rpki.left_right.list_resources_elt, rpki.left_right.list_roa_requests_elt, rpki.left_right.list_published_objects_elt, rpki.left_right.report_error_elt, rpki.publication.con g_elt, rpki.publication.client_elt, rpki.publication.publication_object_elt, and rpki.publication.report_error_elt.

De nition at line 135 of le xml_utils.py.

10.202.3.2 rpki::xml_utils.base_elt::booleans = () [static]

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

Reimplemented in rpki.left_right.self_elt, rpki.left_right.bsc_elt, rpki.left_right.parent_elt, and rpki.left_right.child_elt.

De nition at line 143 of le xml_utils.py.

10.202.3.3 rpki::xml_utils.base_elt::elements = () [static]

XML elements contained by this element.

Reimplemented in rpki.left_right.self_elt, rpki.left_right.bsc_elt, rpki.left_right.repository_elt, rpki.left_right.parent_elt, rpki.left_right.child_elt, rpki.publication.config_elt, and rpki.publication.client_elt.

Definition at line 139 of file xml_utils.py.

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

- xml_utils.py (2836)

10.203 rpki.xml_utils.data_elt Class Reference

Inherits rpki::xml_utils::base_elt.

Inherited by rpki.left_right.data_elt, and rpki.publication.control_elt.

Public Member Functions

- def endElement
- def make_reply
- def make_reply_clone_hook
- def serve_create
- def serve_destroy
- def serve_destroy_hook
- def serve_dispatch
- def serve_fetch_one
- def serve_get
- def serve_list
- def serve_post_save_hook
- def serve_pre_save_hook
- def serve_set
- def toXML
- def unimplemented_control

10.203.1 Detailed Description

Virtual base class for PDUs that map to SQL objects. These objects all implement the create/set/get/list/destroy action attribute.

Definition at line 243 of file xml_utils.py.

10.203.2 Member Function Documentation

10.203.2.1 def rpki.xml_utils.data_elt.endElement (self, stack, name, text)

Default endElement handler for SQL-based objects. This assumes that sub-elements are Base64-encoded using the sql_template mechanism.

Reimplemented from rpki.xml_utils.base_elt.

Reimplemented in rpki.left_right.child_elt, and rpki.publication.client_elt.

Definition at line 249 of file xml_utils.py.

10.203.2.2 def rpki.xml_utils.data_elt.make_reply (self, r_pdu = None)

Construct a reply PDU.

Definition at line 275 of file xml_utils.py.

10.203.2.3 def rpki.xml_utils.data_elt.make_reply_clone_hook (self, r_pdu)

Overridable hook.

Reimplemented in rpki.left_right.data_elt.

Definition at line 292 of file xml_utils.py.

10.203.2.4 def rpki.xml_utils.data_elt.serve_creates (self, r_msg, cb, eb)

Handle a create action.

Definition at line 314 of file xml_utils.py.

10.203.2.5 def rpki.xml_utils.data_elt.serve_destroys (self, r_msg, cb, eb)

Handle a destroy action.

Definition at line 384 of file xml_utils.py.

10.203.2.6 def rpki.xml_utils.data_elt.serve_destroy_hooks(self, cb, eb)

Overridable hook.

Reimplemented in rpki.left_right.child_elt.

De nition at line 378 of le xml_utils.py.

10.203.2.7 def rpki.xml_utils.data_elt.serve_dispatch(self, r_msg, cb, eb)

Action dispatch handler.

Reimplemented in rpki.publication.control_elt.

De nition at line 395 of le xml_utils.py.

10.203.2.8 def rpki.xml_utils.data_elt.serve_fetch_one(self)

Find the object on which a get, set, or destroy method should operate.

De nition at line 296 of le xml_utils.py.

10.203.2.9 def rpki.xml_utils.data_elt.serve_get(self, r_msg, cb, eb)

Handle a get action.

De nition at line 360 of le xml_utils.py.

10.203.2.10 def rpki.xml_utils.data_elt.serve_list(self, r_msg, cb, eb)

Handle a list action for non-self objects.

De nition at line 369 of le xml_utils.py.

10.203.2.11 def rpki.xml_utils.data_elt.serve_post_save_hooks(self, q_pdu, r_pdu, cb, eb)

Overridable hook.

Reimplemented in rpki.left_right.self_elt, rpki.left_right.parent_elt, rpki.left_right.child_elt, and rpki.publication.client_elt.

De nition at line 310 of le xml_utils.py.

10.203.2.12 def rpki.xml_utils.data_elt.serve_pre_save_hooks(self, q_pdu, r_pdu, cb, eb)

Overridable hook.

Reimplemented in rpki.left_right.data_elt and rpki.left_right.bsc_elt.

De nition at line 306 of le xml_utils.py.

10.203.2.13 def rpki.xml_utils.data_elt.serve_sets(self, r_msg, cb, eb)

Handle a set action.

Reimplemented in rpki.publication.con g_elt.

De nition at line 337 of le xml_utils.py.

10.203.2.14 def rpki.xml_utils.data_elt.toXML (self)

Default element generator for SQL-based objects. This assumes that sub-elements are Base64-encoded DER objects.

Reimplemented from rpki.xml_utils.base_elt.

De nition at line 263 of le xml_utils.py.

10.203.2.15 def rpki.xml_utils.data_elt.unimplemented_control (self, controls)

Uniform handling for unimplemented control operations.

Definition at line 408 of file xml_utils.py.

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

- xml_utils.py (2836)

10.204 rpki.xml_utils.msg Class Reference

Inherits list.

Inherited by rpki.left_right.msg, and rpki.publication.msg

Public Member Functions

- def __str__
- def endElement
- def is_query
- def is_reply
- def query
- def reply
- def startElement
- def toXML

Public Attributes

- type
- version

10.204.1 Detailed Description

Generic top-level PDU.

Definition at line 416 of file xml_utils.py.

10.204.2 Member Function Documentation

10.204.2.1 def rpki.xml_utils.msg.__str__(self)

Convert msg object to string.

De nition at line 442 of le xml_utils.py.

10.204.2.2 def rpki.xml_utils.msg.endElement(self, stack, name, text)

Handle top-level PDU.

De nition at line 434 of le xml_utils.py.

10.204.2.3 def rpki.xml_utils.msg.is_query(self)

Is this msg a query?

De nition at line 468 of le xml_utils.py.

10.204.2.4 def rpki.xml_utils.msg.is_reply(self)

Is this msg a reply?

De nition at line 472 of le xml_utils.py.

10.204.2.5 def rpki.xml_utils.msg.query(cls, args)

Create a query PDU.

De nition at line 455 of le xml_utils.py.

10.204.2.6 def rpki.xml_utils.msg.reply (cls, args)

Create a reply PDU.

De nition at line 462 of le xml_utils.py.

10.204.2.7 def rpki.xml_utils.msg.startElement (self, stack, name, attrs)

Handle top-level PDU.

De nition at line 421 of le xml_utils.py.

10.204.2.8 def rpki.xml_utils.msg.toXML (self)

Generate top-level PDU.

De nition at line 446 of le xml_utils.py.

10.204.3 Member Data Documentation

10.204.3.1 rpki.xml_utils.msg.type

De nition at line 427 of le xml_utils.py.

10.204.3.2 rpki.xml_utils.msg.version

Reimplemented in rpki.left_right.msg and rpki.publication.msg

De nition at line 426 of le xml_utils.py.

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

- xml_utils.py (2836)

10.205 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

10.205.1 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.

De nition at line 38 of le xml_utils.py.

10.205.2 Member Function Documentation

10.205.2.1 def rpki.xml_utils.sax_handler.__init__ (self)

Initialize SAX handler.

De nition at line 53 of le xml_utils.py.

10.205.2.2 def rpki.xml_utils.sax_handler.characters(self, content)

Accumulate a chuck of element content (text).

De nition at line 69 of le xml_utils.py.

10.205.2.3 def rpki.xml_utils.sax_handler.create_top_level(self, name, attrs)

Handle top-level PDU for this protocol.

De nition at line 119 of le xml_utils.py.

10.205.2.4 def rpki.xml_utils.sax_handler.endElement(self, name)

Handle endElement() events. Mostly this means handling any accumulated element text.

De nition at line 101 of le xml_utils.py.

10.205.2.5 def rpki.xml_utils.sax_handler.endElementNS(self, name, qname)

Redirect endElementNS() events to endElement().

De nition at line 65 of le xml_utils.py.

10.205.2.6 def rpki.xml_utils.sax_handler.saxify(cls, elt)

Create a one-off SAX parser, parse an ETree, return the result.

De nition at line 111 of le xml_utils.py.

10.205.2.7 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.

De nition at line 73 of le xml_utils.py.

10.205.2.8 def rpki.xml_utils.sax_handler.startElementNS (self, name, qname, attrs)

Redirect startElementNS() events to startElement().

De nition at line 61 of le xml_utils.py.

10.205.3 Member Data Documentation

10.205.3.1 rpki.xml_utils.sax_handler.result

De nition at line 97 of le xml_utils.py.

10.205.3.2 rpki.xml_utils.sax_handler.stack

De nition at line 59 of le xml_utils.py.

10.205.3.3 rpki.xml_utils.sax_handler.text

De nition at line 58 of le xml_utils.py.

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

- xml_utils.py (2836)

10.206 rpki.xml_utils.text_elt Class Reference

Inherits rpki::xml_utils::base_elt.

Inherited by rpki.left_right.list_published_objects_elt, rpki.left_right.report_error_elt, and rpki.publication.report_error_elt.

Public Member Functions

- def endElement
- def toXML

Static Public Attributes

- text_attribute = None

  Name of the class attribute that holds the text value.

10.206.1 Detailed Description

Virtual base class for XML message elements that contain text.

Definition at line 219 of file xml_utils.py.

10.206.2 Member Function Documentation

10.206.2.1 def rpki.xml_utils.text_elt.endElement (self, stack, name, text)

Extract text from parsed XML.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 228 of file xml_utils.py.

10.206.2.2 def rpki.xml_utils.text_elt.toXML (self)

Insert text into generated XML.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 235 of file xml_utils.py.

10.206.3 Member Data Documentation

10.206.3.1 rpki::xml_utils.text_elt::text_attribute = None [static]

Name of the class attribute that holds the text value.

Reimplemented in rpki.left_right.list_published_objects_elt, rpki.left_right.report_error_elt, and rpki.publication.report_error_elt.

De nition at line 226 of le xml_utils.py.

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

- xml_utils.py (2836)

10.207 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 le:

- roa.py (2424)

10.208 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 le:

- roa.py (2424)

10.209 TextWrapper Class Reference

Inherited by irbe_cli.UsageWrapper.

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

- irbe_cli.py (2799)

10.210 ContentHandler Class Reference

Inherited by rpki.xml_utils.sax_handler.

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

- xml_utils.py (2836)

11 File Documentation

11.1 __init__.py File Reference

Packages

- package rpki

11.2 async.py File Reference

Classes

- class rpki.async.gc_summary
- class rpki.async.iterator
- class rpki.async.sync_wrapper
- class rpki.async.timer

Packages

- package rpki.async

Functions

- def rpki::async._raiseExitNow
- def rpki::async.defer
- def rpki::async.event_loop
- def rpki::async.exit_event_loop
- def rpki::async.run_deferred

Variables

- list rpki::async.deferred_queue = [ ]

  List to hold deferred actions.

- rpki::async.ExitNow= asyncore.ExitNow

11.3 con g.py File Reference

Classes

- classrpki.con g.parser

Packages

- packagerpki.con g

11.4 exceptions.py File Reference

Classes

- classrpki.exceptions.BadClassNameSyntax
- classrpki.exceptions.BadClientURL
- classrpki.exceptions.BadContactURL
- classrpki.exceptions.BadExtension
- classrpki.exceptions.BadIRDBReply
- classrpki.exceptions.BadIssueResponse
- classrpki.exceptions.BadPKCS10
- classrpki.exceptions.BadPublicationReply
- classrpki.exceptions.BadQuery
- classrpki.exceptions.BadSender
- classrpki.exceptions.BadStatusCode
- classrpki.exceptions.BadURISyntax
- classrpki.exceptions.BSCNotFound
- classrpki.exceptions.BSCNotReady
- classrpki.exceptions.ChildNotFound
- classrpki.exceptions.ClassNameMismatch
- classrpki.exceptions.ClassNameUnknown
- classrpki.exceptions.ClientNotFound
- classrpki.exceptions.CMSContentNotSet
- classrpki.exceptions.CMSCRLNotSet
- classrpki.exceptions.CMSVeri cationFailed
- classrpki.exceptions.DBConsistancyError
- classrpki.exceptions.DERObjectConversionError
- classrpki.exceptions.DuplicateObject
- classrpki.exceptions.EmptyPEM

- classrpki.exceptions.EmptyROAPre xList
- classrpki.exceptions.ForbiddenURI
- classrpki.exceptions.HandleTranslationError
- classrpki.exceptions.HTTPRequestFailed
- classrpki.exceptions.HTTPSBadVersion
- classrpki.exceptions.HTTPSClientAborted
- classrpki.exceptions.HTTPSUnexpectedState
- classrpki.exceptions.MissingCMSCRL
- classrpki.exceptions.MissingCMSEEcert
- classrpki.exceptions.MultipleTLSEECert
- classrpki.exceptions.MustBePre x
- classrpki.exceptions.NoActiveCA
- classrpki.exceptions.NoCoveringCertForROA
- classrpki.exceptions.NoObjectAtURI
- classrpki.exceptions.NotACerti cateChain
- classrpki.exceptions.NotFound
- classrpki.exceptions.NotImplementedYet
- classrpki.exceptions.NotInDatabase
- classrpki.exceptions.ReceivedTLSCACert
- classrpki.exceptions.RPKI_Exception
- classrpki.exceptions.ServerShuttingDown
- classrpki.exceptions.SKIMismatch
- classrpki.exceptions.SubprocessError
- classrpki.exceptions.TLSValidationError
- classrpki.exceptions.UnexpectedCMSCerts
- classrpki.exceptions.UnexpectedCMSCRLs
- classrpki.exceptions.UnparsableCMSDER
- classrpki.exceptions.UpstreamError
- classrpki.exceptions.WrongEContentType

Packages

- packagerpki.exceptions

11.5 https.py File Reference

Classes

- classrpki.https.http_client
- classrpki.https.http_listener
- classrpki.https.http_message
- classrpki.https.http_queue

- class rpki.https.http_request
- class rpki.https.http_response
- class rpki.https.http_server
- class rpki.https.http_stream

Packages

- package rpki.https

Functions

- def rpki::https.build_https_ta_cache
- def rpki::https.client
- def rpki::https.log_method
- def rpki::https.server

Variables

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

11.6 ipaddrs.py File Reference

Classes

- class rpki.ipaddrs.v4addr
- class rpki.ipaddrs.v6addr

Packages

- package rpki.ipaddrs

11.7 irbe_cli.py File Reference

Classes

- class irbe_cli.bsc_elt
- class irbe_cli.caller
- class irbe_cli.certi cate_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.con g_elt
- class irbe_cli.crl_elt
- class irbe_cli.left_right_cms_msg
- class irbe_cli.left_right_msg
- class irbe_cli.left_right_sax_handler
- class irbe_cli.list_published_objects_elt
- class irbe_cli.manifest_elt
- class irbe_cli.parent_elt
- class irbe_cli.publication_cms_msg
- class irbe_cli.publication_msg
- class irbe_cli.publication_sax_handler
- class irbe_cli.reply_elt_mixin
- class irbe_cli.report_error_elt
- class irbe_cli.report_error_elt
- class irbe_cli.repository_elt
- class irbe_cli.roa_elt
- class irbe_cli.self_elt
- class irbe_cli.UsageWrapper

Packages

- package irbe_cli

Functions

- def irbe_cli.usage

Variables

- list irbe_cli.argv = sys.argv[1:]
- tuple irbe_cli.call_pubd
- tuple irbe_cli.call_rpkid
- tuple irbe_cli.cfg = rpki.con g.parser(cfg_ le, "irbe_cli")
- string irbe_cli.cfg_ le = "irbe.conf"
- irbe_cli.pem_out = None
- irbe_cli.q_msg = q_msg_left_right
- tuple irbe_cli.q_msg_left_right = left_right_msg.query()
- tuple irbe_cli.q_msg_publication = publication_msg.query()
- list irbe_cli.q_pdu = left_right_msg.pdus[argv[0]]
- list irbe_cli.top_opts = ["con g=", "help", "pem_out=", "quiet", "verbose"]
- tuple irbe_cli.usage_ ll = UsageWrapper(subsequent_indent = "4")
- irbe_cli.verbose = True

11.8 irdbd.py File Reference

Packages

- package irdbd

Functions

- def irdbd.handle_list_resources
- def irdbd.handle_list_roa_requests
- def irdbd.handler

Variables

- tuple irdbd.bpki_ta = rpki.x509.X509(Auto_ le = cfg.get("bpki-ta"))
- tuple irdbd.cfg = rpki.con g.parser(cfg_ le, "irdbd")
- string irdbd.cfg_ le = "irdbd.conf"
- tuple irdbd.client_ta = (bpki_ta, rpkid_cert)
- tuple irdbd.cur = db.cursor()
- tuple irdbd.db
- dictionary irdbd.handle_dispatch
- tuple irdbd.handlers = ((u.path, handler),)
- string irdbd.host = "localhost"
- tuple irdbd.irdbd_cert = rpki.x509.X509(Auto_ le = cfg.get("irdbd-cert"))
- tuple irdbd.irdbd_key = rpki.x509.RSA(Auto_ le = cfg.get("irdbd-key"))
- int irdbd.port = 443

- tuple irdbd.rpkid_cert = rpki.x509.X509(Auto_ le = cfg.get("rpkid-cert"))
- irdbd.server_cert = irdbd_cert,
- tuple irdbd.startup_msg = cfg.get("startup-message", "")
- tuple irdbd.u = urlparse.urlparse(cfg.get("https-url"))

11.9 left_right.py File Reference

Classes

- class rpki.left_right.bsc_elt
- class rpki.left_right.child_elt
- class rpki.left_right.cms_msg
- class rpki.left_right.data_elt
- class rpki.left_right.left_right_namespace
- class rpki.left_right.list_published_objects_elt
- class rpki.left_right.list_resources_elt
- class rpki.left_right.list_roa_requests_elt
- class rpki.left_right.msg
- class rpki.left_right.parent_elt
- class rpki.left_right.report_error_elt
- class rpki.left_right.repository_elt
- class rpki.left_right.sax_handler
- class rpki.left_right.self_elt

Packages

- package rpki.left_right

Variables

- rpki::left_right.enforce_strict_up_down_xml_sender = False

11.10 log.py File Reference

Classes

- class rpki.log.logger

Packages

- package rpki.log

Functions

- def rpki::log.init
- def rpki::log.set_trace
- def rpki::log.trace
- def rpki::log.traceback

Variables

- tuple rpki::log.debug = logger(syslog.LOG_DEBUG)
- rpki::log.enable_trace = False

  Whether call tracing is enabled.

- tuple rpki::log.error = logger(syslog.LOG_ERR)
- tuple rpki::log.info = logger(syslog.LOG_INFO)
- tuple rpki::log.note = logger(syslog.LOG_NOTICE)
- int rpki::log.pid = 0
- string rpki::log.tag = ""
- rpki::log.use_syslog = True

  Whether to use syslog.

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

11.11 manifest.py File Reference

Classes

- class rpki.manifest.FileAndHash
- class rpki.manifest.FilesAndHashes
- class rpki.manifest.Manifest

Packages

- package rpki.manifest

11.12 oids.py File Reference

Packages

- package rpki.oids

Variables

- tuple rpki::oids.name2oid = dict((v, k) for k, v in oid2name.items())
  Mapping table of string names to OIDs.
- dictionary rpki::oids.oid2name
  Mapping table of OIDs to conventional string names.

11.13 pubd.py File Reference

Classes

- class pubd.pubd_context

Packages

- package pubd

Functions

- def pubd.main

Variables

- string pubd.cfg_ le = "pubd.conf"
- pubd.pro le = False

11.14 publication.py File Reference

Classes

- class rpki.publication.certi cate_elt
- class rpki.publication.client_elt
- class rpki.publication.cms_msg
- class rpki.publication.con g_elt
- class rpki.publication.control_elt
- class rpki.publication.crl_elt
- class rpki.publication.manifest_elt
- class rpki.publication.msg
- class rpki.publication.publication_namespace

- class rpki.publication.publication_object_elt
- class rpki.publication.report_error_elt
- class rpki.publication.roa_elt
- class rpki.publication.sax_handler

Packages

- package rpki.publication

11.15 relaxng.py File Reference

Packages

- package rpki.relaxng

Variables

- tuple rpki::relaxng.left_right
  Parsed RelaxNG left_right schema.
- tuple rpki::relaxng.publication
  Parsed RelaxNG publication schema.
- tuple rpki::relaxng.up_down
  Parsed RelaxNG up_down schema.

11.16 resource_set.py File Reference

Classes

- class rpki.resource_set.resource_bag
- class rpki.resource_set.resource_range
- class rpki.resource_set.resource_range_as
- class rpki.resource_set.resource_range_ip
- class rpki.resource_set.resource_range_ipv4
- class rpki.resource_set.resource_range_ipv6
- class rpki.resource_set.resource_set
- class rpki.resource_set.resource_set_as
- class rpki.resource_set.resource_set_ip
- class rpki.resource_set.resource_set_ipv4

- class rpki.resource_set.resource_set_ipv6
- class rpki.resource_set.roa_pre x
- class rpki.resource_set.roa_pre x_ipv4
- class rpki.resource_set.roa_pre x_ipv6
- class rpki.resource_set.roa_pre x_set
- class rpki.resource_set.roa_pre x_set_ipv4
- class rpki.resource_set.roa_pre x_set_ipv6

Packages

- package rpki.resource_set

Functions

- def rpki::resource_set._bs2long
- def rpki::resource_set._long2bs
- def rpki::resource_set._rsplit
- def rpki::resource_set.test1
- def rpki::resource_set.test2

Variables

- string rpki::resource_set.inherit_token = "<inherit>"

  Token used to indicate inheritance in read and print syntax.

11.17 roa.py File Reference

Classes

- class rpki.roa.ROAIPAddress
- class rpki.roa.ROAIPAddresses
- class rpki.roa.ROAIPAddressFamilies
- class rpki.roa.ROAIPAddressFamily
- class rpki.roa.RouteOriginAttestation

Packages

- package rpki.roa

11.18 rootd.py File Reference

Classes

- class rootd.cms_msg
- class rootd.issue_pdu
- class rootd.list_pdu
- class rootd.message_pdu
- class rootd.revoke_pdu
- class rootd.sax_handler

Packages

- package rootd

Functions

- def rootd.compose_response
- def rootd.del_subject_cert
- def rootd.del_subject_pkcs10
- def rootd.get_root_cert
- def rootd.get_subject_cert
- def rootd.get_subject_pkcs10
- def rootd.issue_subject_cert_maybe
- def rootd.root_newer_than_subject
- def rootd.set_subject_cert
- def rootd.set_subject_pkcs10
- def rootd.up_down_handler

Variables

- tuple rootd.bpki_ta = rpki.x509.X509(Auto_ le = cfg.get("bpki-ta"))
- tuple rootd.cfg = rpki.con g.parser(cfg_ le, "rootd")
- string rootd.cfg_ le = "rootd.conf"
- tuple rootd.child_bpki_cert = rpki.x509.X509(Auto_ le = 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_ le = cfg.get("rootd-bpki-cert"))
- tuple rootd.rootd_bpki_crl = rpki.x509.CRL(Auto_ le = cfg.get("rootd-bpki-crl"))
- tuple rootd.rootd_bpki_key = rpki.x509.RSA(Auto_ le = cfg.get("rootd-bpki-key"))
- tuple rootd.rpki_base_uri = cfg.get("rpki-base-uri", "rsync://" + rpki_class_name + ".invalid/")
- tuple rootd.rpki_class_name = cfg.get("rpki-class-name", "wombat")
- rootd.rpki_root_cert = None
- tuple rootd.rpki_root_cert_ le = 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_ le = cfg.get("rpki-root-key"))
- tuple rootd.rpki_root_manifest = cfg.get("rpki-root-manifest", "Root.mnf")
- tuple rootd.rpki_subject_cert = cfg.get("rpki-subject-cert", "Child.cer")
- tuple rootd.rpki_subject_lifetime = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-lifetime", "30d"))
- tuple rootd.rpki_subject_pkcs10 = cfg.get("rpki-subject-pkcs10", "Child.pkcs10")
- tuple rootd.rpki_subject_regen = rpki.sundial.timedelta.parse(cfg.get("rpki-subject-regen", rpki_subject_lifetime.convert_to_seconds() / 2))
- rootd.server_cert = rootd_bpki_cert,

11.19 rpki_engine.py File Reference

Classes

- class rpki.rpki_engine.ca_detail_obj
- class rpki.rpki_engine.ca_obj
- class rpki.rpki_engine.child_cert_obj
- class rpki.rpki_engine.publication_queue
- class rpki.rpki_engine.revoked_cert_obj
- class rpki.rpki_engine.roa_obj
- class rpki.rpki_engine.rpkid_context

Packages

- package rpki.rpki_engine

11.20 rpkid.py File Reference

Packages

- package rpkid

Functions

- def rpkid.main

Variables

- string rpkid.cfg_ le = "rpkid.conf"
- rpkid.pro le = None

11.21 sql.py File Reference

Classes

- class rpki.sql.session
- class rpki.sql.sql_persistent
- class rpki.sql.template

Packages

- package rpki.sql

11.22 sundial.py File Reference

Classes

- class rpki.sundial.datetime
- class rpki.sundial.timedelta

Packages

- package rpki.sundial

Functions

- def rpki::sundial._cast
- def rpki::sundial.now
- def rpki::sundial.test

11.23 up_down.py File Reference

Classes

- class rpki.up_down.base_elt
- class rpki.up_down.certi cate_elt
- class rpki.up_down.class_elt
- class rpki.up_down.class_response_syntax
- class rpki.up_down.cms_msg
- class rpki.up_down.error_response_pdu
- class rpki.up_down.issue_pdu
- class rpki.up_down.issue_response_pdu
- class rpki.up_down.list_pdu
- class rpki.up_down.list_response_pdu
- class rpki.up_down.message_pdu
- class rpki.up_down.multi_uri
- class rpki.up_down.revoke_pdu
- class rpki.up_down.revoke_response_pdu
- class rpki.up_down.revoke_syntax
- class rpki.up_down.sax_handler

Packages

- package rpki.up_down

Variables

- dictionary rpki::up_down.nsmap = { None : xmlns }
- string rpki::up_down.xmlns = "http://www.apnic.net/specs/rescerts/up-down/"

11.24 x509.py File Reference

Classes

- class rpki.x509.CMS_object
- class rpki.x509.CRL

- class rpki.x509.DeadDrop
- class rpki.x509.DER_CMS_object
- class rpki.x509.DER_object
- class rpki.x509.PEM_converter
- class rpki.x509.PKCS10
- class rpki.x509.ROA
- class rpki.x509.RSA
- class rpki.x509.RSApublic
- class rpki.x509.SignedManifest
- class rpki.x509.X509
- class rpki.x509.XML_CMS_object

Packages

- package rpki.x509

Functions

- def rpki::x509.calculate_SKI
- def rpki::x509.POWify_OID

11.25 xml_utils.py File Reference

Classes

- class rpki.xml_utils.base_elt
- class rpki.xml_utils.data_elt
- class rpki.xml_utils.msg
- class rpki.xml_utils.sax_handler
- class rpki.xml_utils.text_elt

Packages

- package rpki.xml_utils

Index

__abs__
rpki::sundial::timedelta, 330
__add__
rpki::sundial::datetime, 325
rpki::sundial::timedelta, 330
__call__
irbe_cli::caller, 98
irbe_cli::UsageWrapper, 113
rpki::async::iterator, 125
rpki::async::sync_wrapper, 127
rpki::log::logger, 221
__cmp__
rpki::async::timer, 130
rpki::resource_set::resource_range, 251
rpki::resource_set::roa_pre x, 265
rpki::x509::DER_object, 372
__del__
rpki::async::timer, 130
__div__
rpki::sundial::timedelta, 330
__eq__
rpki::resource_set::resource_bag, 247
__ oordiv__
rpki::sundial::timedelta, 330
__init__
irbe_cli::caller, 98
pubd::pubd_context, 115
rpki::async::gc_summary, 123
rpki::async::iterator, 125
rpki::async::sync_wrapper, 127
rpki::async::timer, 130
rpki::con g::parser, 134
rpki::https::http_client, 156
rpki::https::http_listener, 160
rpki::https::http_message, 163
rpki::https::http_queue, 165
rpki::https::http_request, 168
rpki::https::http_response, 169
rpki::https::http_server, 171
rpki::https::http_stream, 175
rpki::log::logger, 221
rpki::manifest::FileAndHash, 222
rpki::manifest::FilesAndHashes, 223
rpki::manifest::Manifest, 224
rpki::resource_set::resource_bag, 247
rpki::resource_set::resource_range, 251
rpki::resource_set::resource_set, 257
rpki::resource_set::roa_pre x, 266
rpki::resource_set::roa_pre x_set, 269
rpki::roa::ROAIPAddress, 273
rpki::roa::ROAIPAddresses, 274
rpki::roa::ROAIPAddressFamilies, 275
rpki::roa::ROAIPAddressFamily, 275
rpki::roa::RouteOriginAttestation, 276
rpki::rpki_engine::child_cert_obj, 292
rpki::rpki_engine::publication_-queue, 296
rpki::rpki_engine::revoked_cert_obj, 298
rpki::rpki_engine::roa_obj, 301
rpki::rpki_engine::rpkid_context, 307
rpki::sql::session, 313
rpki::sql::template, 323
rpki::up_down::class_elt, 338
rpki::up_down::class_response_-syntax, 341
rpki::up_down::error_response_pdu, 343
rpki::up_down::multi_uri, 354
rpki::x509::DeadDrop, 368
rpki::x509::DER_object, 372
rpki::x509::PEM_converter, 378
rpki::xml_utils::sax_handler, 409
__init__.py(2937), 414

__mul__
rpki::sundial::timedelta, 330
__ne__
rpki::resource_set::resource_bag, 248
__neg__
rpki::sundial::timedelta, 330
__new__
rpki::ipaddrs::v4addr, 180
rpki::ipaddrs::v6addr, 181
__pos__
rpki::sundial::timedelta, 330
__radd__
rpki::sundial::datetime, 325
rpki::sundial::timedelta, 330
__rdiv__
rpki::sundial::timedelta, 331
__repr__
rpki::async::iterator, 125
rpki::async::timer, 130
__r oordiv__
rpki::sundial::timedelta, 331
__rmul__
rpki::sundial::timedelta, 331
__rsub__
rpki::sundial::datetime, 325
rpki::sundial::timedelta, 331
__str__
rpki::https::http_message, 163
rpki::ipaddrs::v4addr, 180
rpki::ipaddrs::v6addr, 181
rpki::publication::report_error_elt, 243
rpki::resource_set::resource_bag, 248
rpki::resource_set::resource_range_as, 252
rpki::resource_set::resource_range_ip, 254
rpki::resource_set::resource_set, 257
rpki::resource_set::roa_pre x, 266
rpki::resource_set::roa_pre x_set, 269
rpki::sundial::datetime, 325
rpki::up_down::message_pdu, 351
rpki::up_down::multi_uri, 354
rpki::xml_utils::base_elt, 399
rpki::xml_utils::msg, 407
__sub__
rpki::sundial::datetime, 325
rpki::sundial::timedelta, 331
_add
rpki::rpki_engine::publication_queue, 296
_bs2long
rpki::resource_set, 83
_cast
rpki::sundial, 88
_comm
rpki::resource_set::resource_set, 257
_exceptions_enabled
rpki::sql::session, 315
_get_wrapper
rpki::con g::parser, 134
_long2bs
rpki::resource_set, 83
_pre xlen
rpki::resource_set::resource_range_ip, 254
_raiseExitNow
rpki::async, 64
_rsplit
rpki::resource_set, 83
_wrap_execute
rpki::sql::session, 313

activate
rpki::rpki_engine::ca_detail_obj, 279
address
rpki::roa::ROAIPAddress, 273
addresses
rpki::roa::ROAIPAddressFamily, 276
addressFamily
rpki::roa::ROAIPAddressFamily, 276
a
rpki::resource_set::resource_set_ipv4, 263
rpki::resource_set::resource_set_ipv6, 264

argv
irbe_cli, 47
asID
rpki::roa::RouteOriginAttestation, 277
asn
rpki::left_right::list_resources_elt, 198
rpki::resource_set::resource_bag, 249
rpki::rpki_engine::roa_obj, 304
assert_pristine
rpki::sql::session, 313
async.py(2926), 414
asynchat::async_chat, 85
asyncore::dispatcher, 95
attributes
rpki::left_right::bsc_elt, 184
rpki::left_right::child_elt, 188
rpki::left_right::list_published_objects_elt, 196
rpki::left_right::list_resources_elt, 198
rpki::left_right::list_roa_requests_elt, 200
rpki::left_right::parent_elt, 205
rpki::left_right::report_error_elt, 208
rpki::left_right::repository_elt, 211
rpki::left_right::self_elt, 219
rpki::publication::client_elt, 228
rpki::publication::con g_elt, 233
rpki::publication::publication_object_elt, 241
rpki::publication::report_error_elt, 243
rpki::xml_utils::base_elt, 401

b
rpki::x509::PEM_converter, 378
base_uri
rpki::publication::client_elt, 228
bits
rpki::ipaddrs::v4addr, 180
rpki::ipaddrs::v6addr, 182
body
rpki::https::http_message, 164
booleans
rpki::left_right::bsc_elt, 184
rpki::left_right::child_elt, 188
rpki::left_right::parent_elt, 205
rpki::left_right::self_elt, 219
rpki::xml_utils::base_elt, 401
bpki_cert
irbe_cli::cmd_elt_mixin, 102
rpki::left_right::child_elt, 189
rpki::left_right::repository_elt, 211
rpki::left_right::self_elt, 219
rpki::publication::client_elt, 228
bpki_cms_cert
irbe_cli::cmd_elt_mixin, 102
rpki::left_right::parent_elt, 205
bpki_cms_glue
irbe_cli::cmd_elt_mixin, 102
rpki::left_right::parent_elt, 206
bpki_crl
irbe_cli::con g_elt, 105
bpki_glue
irbe_cli::cmd_elt_mixin, 103
rpki::left_right::child_elt, 189
rpki::left_right::repository_elt, 211
rpki::left_right::self_elt, 219
rpki::publication::client_elt, 229
bpki_https_cert
irbe_cli::cmd_elt_mixin, 103
rpki::left_right::parent_elt, 206
bpki_https_glue
irbe_cli::cmd_elt_mixin, 103
rpki::left_right::parent_elt, 206
bpki_ta
irdbd, 51
pubd::pubd_context, 116
rootd, 58
rpki::rpki_engine::rpkid_context, 309
bsc
rpki::left_right::data_elt, 192
bscs
rpki::left_right::self_elt, 215
buffer
rpki::https::http_stream, 178
build
rpki::x509::ROA, 382

rpki::x509::SignedManifest, 389
build_https_ta_cache
pubd::pubd_context, 115
rpki::https, 69
rpki::rpki_engine::rpkid_context, 307
ca
rpki::rpki_engine::ca_detail_obj, 279
ca_cert_uri
rpki::rpki_engine::ca_detail_obj, 283
ca_detail
rpki::rpki_engine::child_cert_obj, 292
rpki::rpki_engine::revoked_cert_obj, 298
rpki::rpki_engine::roa_obj, 301
ca_detail_id
rpki::rpki_engine::child_cert_obj, 294
rpki::rpki_engine::revoked_cert_obj, 299
rpki::rpki_engine::roa_obj, 304
ca_details
rpki::rpki_engine::ca_obj, 287
ca_from_class_name
rpki::left_right::child_elt, 187
ca_id
rpki::rpki_engine::ca_detail_obj, 283
cache
rpki::sql::session, 315
cache_clear
rpki::sql::session, 314
calculate_SKI
rpki::x509, 92
call_pubd
irbe_cli, 47
rpki::left_right::repository_elt, 210
rpki::rpki_engine::publication_queue, 296
call_rpkid
irbe_cli, 47
callback
rpki::https::http_request, 168
caller_function
rpki::async::iterator, 126
cancel
rpki::async::timer, 130
cas
rpki::left_right::parent_elt, 204
cb
rpki::async::sync_wrapper, 127
cert
rpki::https::http_client, 158
rpki::https::http_listener, 161
rpki::https::http_queue, 166
rpki::rpki_engine::child_cert_obj, 294
rpki::rpki_engine::roa_obj, 304
rpki::up_down::certi cate_elt, 336
cert_url
rpki::up_down::certi cate_elt, 336
rpki::up_down::class_elt, 339
certs
rpki::up_down::class_elt, 339
cfg
irbe_cli, 47
irdbd, 51
rootd, 58
rpki::con g::parser, 136
cfg_ le
irbe_cli, 47
irdbd, 51
pubd, 54
rootd, 58
rpkid, 94
characters
rpki::xml_utils::sax_handler, 410
check_allowed_uri
rpki::publication::client_elt, 227
check_for_updates
rpki::rpki_engine::ca_obj, 287
check_response
rpki::up_down::base_elt, 333
rpki::up_down::error_response_pdu, 343
rpki::up_down::issue_response_pdu, 348
check_valid_rpki

rpki::x509::PKCS10, 380
checkpoint
rpki::rpki_engine::rpkid_context, 307
child
rpki::rpki_engine::child_cert_obj, 292
child_bpki_cert
rootd, 59
child_certs
rpki::left_right::child_elt, 187
rpki::rpki_engine::ca_detail_obj, 279
child_id
rpki::rpki_engine::child_cert_obj, 294
children
rpki::left_right::bsc_elt, 183
rpki::left_right::self_elt, 215
chunk_body
rpki::https::http_stream, 175
chunk_discard_crlf
rpki::https::http_stream, 175
chunk_discard_trailer
rpki::https::http_stream, 175
chunk_handler
rpki::https::http_stream, 178
chunk_header
rpki::https::http_stream, 175
class_name
rpki::up_down::class_elt, 339
rpki::up_down::issue_pdu, 347
rpki::up_down::revoke_pdu, 356
rpki::up_down::revoke_syntax, 358
classes
rpki::up_down::class_response_-syntax, 341
clear
rpki::async::timer, 130
rpki::x509::DER_object, 372
clear_https_ta_cache
pubd::pubd_context, 115
rpki::left_right::child_elt, 189
rpki::publication::client_elt, 229
rpki::rpki_engine::rpkid_context, 307
client
rpki::https, 70
rpki::https::http_queue, 166
client_cert
irbe_cli::caller, 98
client_getopt
irbe_cli::cmd_elt_mixin, 101
client_handler
pubd::pubd_context, 116
client_key
irbe_cli::caller, 98
client_poll
rpki::left_right::self_elt, 215
client_query_bpki_cert
irbe_cli::cmd_elt_mixin, 101
client_query_bpki_cms_cert
irbe_cli::cmd_elt_mixin, 101
client_query_bpki_crl
irbe_cli::con g_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, 102
client_query_https_glue
irbe_cli::cmd_elt_mixin, 102
client_query_signing_cert
irbe_cli::bsc_elt, 96
client_query_signing_cert_crl
irbe_cli::bsc_elt, 96
client_queues
rpki::https, 70
client_reply_decode
irbe_cli::bsc_elt, 96
irbe_cli::reply_elt_mixin, 111
client_reply_show
irbe_cli::reply_elt_mixin, 111
client_ta
irdbd, 51
rootd, 59
client_url_regexp
pubd::pubd_context, 116
close
rpki::https::http_stream, 175
rpki::sql::session, 314

cmd
rpki::https::http_request, 168
cms_class
irbe_cli::caller, 98
code
rpki::https::http_response, 170
codes
rpki::up_down::error_response_pdu, 344
collect_incoming_data
rpki::https::http_stream, 175
columns
rpki::sql::template, 323
compose_response
rootd, 57
con g.py(2926), 415
con g_id
rpki::publication::con g_elt, 233
connect
rpki::sql::session, 314
construct_sia_uri
rpki::rpki_engine::ca_obj, 287
contains
rpki::resource_set::resource_set, 257
content
rpki::x509::CMS_object, 362
rpki::x509::DER_CMS_object, 370
rpki::x509::XML_CMS_object, 397
content_class
rpki::x509::ROA, 382
rpki::x509::SignedManifest, 390
control_handler
pubd::pubd_context, 116
convert_to_seconds
rpki::sundial::timedelta, 331
create
rpki::rpki_engine::ca_detail_obj, 279
rpki::rpki_engine::ca_obj, 287
rpki::x509::PKCS10, 380
create_ca
rpki::x509::PKCS10, 380
create_top_level
rpki::xml_utils::sax_handler, 410
crl_interval
rpki::left_right::self_elt, 220
crl_published
rpki::rpki_engine::ca_detail_obj, 283
crl_published_callback
rpki::rpki_engine::ca_detail_obj, 279
crl_uri
rpki::rpki_engine::ca_detail_obj, 279
crl_uri_tail
rpki::rpki_engine::ca_detail_obj, 280
cron
rpki::left_right::self_elt, 215
rpki::rpki_engine::rpkid_context, 308
cron_keepalive
rpki::rpki_engine::rpkid_context, 309
cron_period
rpki::rpki_engine::rpkid_context, 310
cron_timeout
rpki::rpki_engine::rpkid_context, 310
cron_timer
rpki::rpki_engine::rpkid_context, 310
cronjob_handler
rpki::rpki_engine::rpkid_context, 308
cross_certify
rpki::x509::X509, 391
cur
irdbd, 51
rpki::sql::session, 315

database
rpki::sql::session, 315
datum_type
rpki::resource_set::resource_range_as, 252
rpki::resource_set::resource_range_ipv4, 255
rpki::resource_set::resource_range_ipv6, 256

db
irdbd, 51
rpki::sql::session, 316
debug
rpki::log, 76
debug_cms_certs
rpki::x509::CMS_object, 362
debug_http
rpki::https, 70
debug_tls_certs
rpki::https, 70
decode
rpki::x509::DER_CMS_object, 370
rpki::x509::XML_CMS_object, 396
default_client_timeout
rpki::https, 71
default_http_version
rpki::https, 71
default_pubd_handler
rpki::left_right::repository_elt, 210
default_section
rpki::con g::parser, 136
default_server_timeout
rpki::https, 71
defer
rpki::async, 64
deferred_queue
rpki::async, 65
del_subject_cert
rootd, 57
del_subject_pkcs10
rootd, 57
delete
rpki::rpki_engine::ca_detail_obj, 280
rpki::rpki_engine::ca_obj, 287
rpki::sql::template, 323
DER
rpki::x509::CMS_object, 362
rpki::x509::CRL, 367
rpki::x509::DER_object, 376
rpki::x509::PKCS10, 381
rpki::x509::RSA, 385
rpki::x509::RSApublic, 387
rpki::x509::X509, 394
description
rpki::up_down::error_response_pdu, 344
detach
rpki::https::http_queue, 165
difference
rpki::resource_set::resource_set, 257
dirty
rpki::sql::session, 316
doit
rpki::async::iterator, 125
done_callback
rpki::async::iterator, 126
dump
rpki::x509::DeadDrop, 368
dump_inbound_cms
rpki::x509::XML_CMS_object, 397
dump_on_verify_failure
rpki::x509::CMS_object, 363
dump_outbound_cms
rpki::x509::XML_CMS_object, 398
dump_to_disk
rpki::x509::XML_CMS_object, 396
dumpasn1
rpki::x509::DER_object, 372
dynamic_ta
rpki::https::http_listener, 161

e
rpki::x509::PEM_converter, 378
earlier
rpki::sundial::datetime, 326
eb
rpki::async::sync_wrapper, 127
econtent_oid
rpki::x509::CMS_object, 363
rpki::x509::ROA, 382
rpki::x509::SignedManifest, 390
rpki::x509::XML_CMS_object, 398
element_name
rpki::left_right::bsc_elt, 184
rpki::left_right::child_elt, 189
rpki::left_right::list_published_-objects_elt, 196
rpki::left_right::list_resources_elt, 199

rpki::left_right::list_roa_requests_-elt, 200
rpki::left_right::parent_elt, 206
rpki::left_right::report_error_elt, 208
rpki::left_right::repository_elt, 211
rpki::left_right::self_elt, 220
rpki::publication::certi cate_elt, 226
rpki::publication::client_elt, 229
rpki::publication::con g_elt, 233
rpki::publication::crl_elt, 235
rpki::publication::manifest_elt, 236
rpki::publication::report_error_elt, 244
rpki::publication::roa_elt, 245
elements
rpki::left_right::bsc_elt, 185
rpki::left_right::child_elt, 189
rpki::left_right::parent_elt, 206
rpki::left_right::repository_elt, 212
rpki::left_right::self_elt, 220
rpki::publication::client_elt, 229
rpki::publication::con g_elt, 233
rpki::xml_utils::base_elt, 401
empty
rpki::resource_set::resource_bag, 248
rpki::x509::DER_object, 372
enable_trace
rpki::log, 76
encode
rpki::x509::DER_CMS_object, 370
rpki::x509::XML_CMS_object, 396
encoding
rpki::left_right::cms_msg, 191
rpki::publication::cms_msg, 230
rpki::up_down::cms_msg, 342
endElement
rpki::left_right::child_elt, 187
rpki::publication::client_elt, 227
rpki::publication::publication_-object_elt, 240
rpki::up_down::base_elt, 333
rpki::up_down::certi cate_elt, 335
rpki::up_down::class_elt, 338
rpki::up_down::error_response_pdu, 343
rpki::up_down::issue_pdu, 346
rpki::xml_utils::base_elt, 399
rpki::xml_utils::data_elt, 403
rpki::xml_utils::msg, 407
rpki::xml_utils::sax_handler, 410
rpki::xml_utils::text_elt, 412
endElementNS
rpki::xml_utils::sax_handler, 410
enforce_strict_up_down_xml_sender
rpki::left_right, 74
err
rpki::async::sync_wrapper, 128
errback
rpki::async::timer, 130, 132
rpki::https::http_request, 168
error
rpki::log, 76
error_code
rpki::left_right::report_error_elt, 209
rpki::publication::report_error_elt, 244
error_text
rpki::left_right::report_error_elt, 209
rpki::publication::report_error_elt, 244
event_loop
rpki::async, 64
Exception, 95
exceptions
rpki::up_down::error_response_pdu, 344
exceptions.py(2907), 415
excludes
irbe_cli::bsc_elt, 96
irbe_cli::cmd_elt_mixin, 103
irbe_cli::list_published_objects_elt, 108
execute
rpki::sql::session, 314
executemany
rpki::sql::session, 314
exit_event_loop
rpki::async, 64
ExitNow
rpki::async, 65
expect_close

rpki::https::http_client, 158
rpki::https::http_server, 172
expired
rpki::x509::X509, 392
expires
rpki::rpki_engine::revoked_cert_obj, 299
explicitVersion
rpki::manifest::Manifest, 224
rpki::roa::RouteOriginAttestation, 277
extract
rpki::x509::CMS_object, 361

fetch
rpki::publication::con g_elt, 232
rpki::rpki_engine::child_cert_obj, 293
fetch_active
rpki::rpki_engine::ca_obj, 288
fetch_deprecated
rpki::rpki_engine::ca_obj, 288
fetch_issue_response_candidates
rpki::rpki_engine::ca_obj, 288
fetch_pending
rpki::rpki_engine::ca_obj, 288
fetch_revoked
rpki::rpki_engine::ca_obj, 288
fetchall
rpki::sql::session, 314
le
rpki::manifest::FileAndHash, 223
leHashAlg
rpki::manifest::Manifest, 224
leList
rpki::manifest::Manifest, 224
lename
rpki::con g::parser, 136
nd_handler
rpki::https::http_server, 171
format
rpki::https::http_message, 163
format_ rst_line
rpki::https::http_request, 168
rpki::https::http_response, 169
formats
rpki::x509::CMS_object, 363
rpki::x509::CRL, 367
rpki::x509::DER_object, 376
rpki::x509::PKCS10, 381
rpki::x509::RSA, 385
rpki::x509::RSApublic, 388
rpki::x509::X509, 394
found_terminator
rpki::https::http_stream, 175
from_bytes
rpki::ipaddrs::v4addr, 180
rpki::ipaddrs::v6addr, 181
from_exception
rpki::left_right::report_error_elt, 208
rpki::publication::report_error_elt, 243
from_resource_bag
rpki::up_down::class_elt, 338
from_rfc3779_tuples
rpki::resource_set::resource_bag, 248
from_sql
rpki::resource_set::resource_set, 258
rpki::resource_set::roa_pre x_set, 270
rpki::sundial::datetime, 326
rpki::x509::DER_object, 372
fromASN1tuple
rpki::sundial::datetime, 326
fromdatetime
rpki::sundial::datetime, 326
fromGeneralizedTime
rpki::sundial::datetime, 326
fromtimedelta
rpki::sundial::timedelta, 331
fromUTCTime
rpki::sundial::datetime, 326
fromXMLtime
rpki::sundial::datetime, 327
func
rpki::async::sync_wrapper, 128

gAKI
rpki::x509::DER_object, 373
gc_debug
rpki::async::timer, 132

gctx
rpki::rpki_engine::ca_detail_obj, 283
rpki::rpki_engine::ca_obj, 290
rpki::rpki_engine::child_cert_obj, 294
rpki::rpki_engine::revoked_cert_obj, 299
rpki::rpki_engine::roa_obj, 304
rpki::sql::sql_persistent, 321
generate
rpki::rpki_engine::roa_obj, 301
rpki::x509::CRL, 365
rpki::x509::RSA, 384
generate_crl
rpki::rpki_engine::ca_detail_obj, 280
generate_manifest
rpki::rpki_engine::ca_detail_obj, 280
generate_manifest_cert
rpki::rpki_engine::ca_detail_obj, 280
get
rpki::con g::parser, 135
get_3779resources
rpki::x509::DER_object, 373
get_AIA
rpki::x509::DER_object, 373
get_AKI
rpki::x509::DER_object, 373
get_Base64
rpki::x509::DER_object, 373
get_basicConstraints
rpki::x509::DER_object, 374
get_buffer
rpki::https::http_stream, 176
get_content
rpki::x509::CMS_object, 361
get_DER
rpki::x509::CMS_object, 361
rpki::x509::CRL, 365
rpki::x509::DER_object, 374
rpki::x509::PKCS10, 380
rpki::x509::RSA, 384
rpki::x509::RSApublic, 387
rpki::x509::X509, 392
get_PEM
rpki::x509::DER_object, 374
get_POW
rpki::x509::CMS_object, 361
rpki::x509::CRL, 366
rpki::x509::RSA, 384
rpki::x509::RSApublic, 387
rpki::x509::X509, 392
get_POWpkix
rpki::x509::CRL, 366
rpki::x509::PKCS10, 380
rpki::x509::X509, 392
get_public_DER
rpki::x509::RSA, 384
get_root_cert
rootd, 57
get_RSApublic
rpki::x509::RSA, 385
get_SIA
rpki::x509::DER_object, 374
get_SKI
rpki::up_down::revoke_pdu, 355
rpki::x509::DER_object, 374
rpki::x509::RSA, 385
rpki::x509::RSApublic, 387
get_subject_cert
rootd, 57
get_subject_pkcs10
rootd, 57
getboolean
rpki::con g::parser, 135
getint
rpki::con g::parser, 135
getIssuer
rpki::x509::CRL, 366
rpki::x509::X509, 392
getNextUpdate
rpki::x509::CRL, 366
rpki::x509::SignedManifest, 389
getNotAfter
rpki::x509::X509, 392
getNotBefore
rpki::x509::X509, 393
getPublicKey
rpki::x509::PKCS10, 380

rpki::x509::X509, 393
getSerial
rpki::x509::X509, 393
getSubject
rpki::x509::X509, 393
getThisUpdate
rpki::x509::CRL, 366
rpki::x509::SignedManifest, 389
gSKI
rpki::x509::DER_object, 375

hAKI
rpki::x509::DER_object, 375
handle_accept
rpki::https::http_listener, 161
handle_body
rpki::https::http_stream, 176
handle_close
rpki::https::http_client, 156
rpki::https::http_stream, 176
handle_connect
rpki::https::http_client, 157
handle_dispatch
irdbd, 51
handle_error
rpki::https::http_client, 157
rpki::https::http_listener, 161
rpki::https::http_stream, 176
handle_list_resources
irdbd, 50
handle_list_roa_requests
irdbd, 50
handle_message
rpki::https::http_client, 157
rpki::https::http_server, 171
handle_no_content_length
rpki::https::http_client, 157
rpki::https::http_server, 171
handle_read
rpki::https::http_stream, 176
handle_timeout
rpki::https::http_client, 157
rpki::https::http_stream, 176
handle_write
rpki::https::http_stream, 176
handler
irdbd, 50
rpki::async::gc_summary, 123
rpki::async::timer, 131, 133
handler_common
pubd::pubd_context, 116
handlers
irdbd, 52
rootd, 59
rpki::https::http_listener, 161
rpki::https::http_server, 172
rpki::rpki_engine::publication_-
queue, 297
handles
rpki::left_right::bsc_elt, 185
rpki::left_right::child_elt, 189
rpki::left_right::data_elt, 194
rpki::left_right::parent_elt, 206
rpki::left_right::repository_elt, 212
rpki::left_right::self_elt, 220
has_option
rpki::con g::parser, 135
has_section
rpki::con g::parser, 135
hash
rpki::manifest::FileAndHash, 223
headers
rpki::https::http_message, 164
host
irdbd, 52
rootd, 59
hostport
rpki::https::http_client, 158
rpki::https::http_queue, 166
hSKI
rpki::x509::DER_object, 375
https.py(2902), 416
https_server_host
pubd::pubd_context, 117
rootd, 59
rpki::rpki_engine::rpkid_context,
310
https_server_port
pubd::pubd_context, 117
rootd, 59
rpki::rpki_engine::rpkid_context,
310

https_ta_cache
pubd::pubd_context, 117
rpki::rpki_engine::rpkid_context, 310

ignore
rpki::async::iterator, 125
index
rpki::sql::template, 323
info
rpki::log, 76
inherit
rpki::resource_set::resource_set, 259
rpki::resource_set::resource_set_as, 261
rpki::resource_set::resource_set_ip, 262
inherit_token
rpki::resource_set, 254
init
rpki::log, 75
initial_delay
rpki::rpki_engine::rpkid_context, 310
initiate_send
rpki::https::http_stream, 177
insert
rpki::sql::template, 323
intersection
rpki::resource_set::resource_bag, 248
rpki::resource_set::resource_set, 258
interval
rpki::async::gc_summary, 124
ipAddrBlocks
rpki::roa::RouteOriginAttestation, 277
ipaddrs.py(2424), 417
ipv4
rpki::left_right::list_resources_elt, 199
rpki::left_right::list_roa_requests_elt, 201
rpki::rpki_engine::roa_obj, 305
ipv6
rpki::left_right::list_resources_elt, 199
rpki::left_right::list_roa_requests_elt, 201
rpki::rpki_engine::roa_obj, 305
irbe_cert
pubd::pubd_context, 117
rpki::rpki_engine::rpkid_context, 311
irbe_cli, 45
argv, 47
call_pubd, 47
call_rpkid, 47
cfg, 47
cfg_ le, 47
pem_out, 47
q_msg, 48
q_msg_left_right, 48
q_msg_publication, 48
q_pdu, 48
top_opts, 48
usage, 46
usage_ ll, 48
verbose, 48
irbe_cli.py(2799), 418
irbe_cli::bsc_elt, 95
client_query_signing_cert, 96
client_query_signing_cert_crl, 96
client_reply_decode, 96
excludes, 96
signing_cert, 97
signing_cert_crl, 97
irbe_cli::caller, 97
__call__, 98
__init__, 98
client_cert, 98
client_key, 98
cms_class, 98
server_cert, 98
server_ta, 98
url, 99
irbe_cli::certi cate_elt, 99
irbe_cli::child_elt, 99
irbe_cli::client_elt, 99
irbe_cli::cmd_elt_mixin, 100
bpki_cert, 102

bpki_cms_cert, 102
bpki_cms_glue, 102
bpki_glue, 103
bpki_https_cert, 103
bpki_https_glue, 103
client_getopt, 101
client_query_bpki_cert, 101
client_query_bpki_cms_cert, 101
client_query_bpki_https_cert, 101
client_query_cms_glue, 101
client_query_glue, 102
client_query_https_glue, 102
excludes, 103
is_cmd, 103
usage, 102
irbe_cli::cmd_msg_mixin, 104
usage, 104
irbe_cli::con g_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
pdus, 106
irbe_cli::left_right_sax_handler, 107
pdu, 107
irbe_cli::list_published_objects_elt, 107
excludes, 108
irbe_cli::manifest_elt, 108
irbe_cli::parent_elt, 108
irbe_cli::publication_cms_msg, 109
saxify, 109
irbe_cli::publication_msg, 109
pdus, 110
irbe_cli::publication_sax_handler, 110
pdu, 110
irbe_cli::reply_elt_mixin, 111
client_reply_decode, 111
client_reply_show, 111
is_cmd, 112
irbe_cli::report_error_elt, 112
irbe_cli::repository_elt, 112
irbe_cli::roa_elt, 112
irbe_cli::self_elt, 113
irbe_cli::UsageWrapper, 113
__call__, 113
irdb_cert
rpki::rpki_engine::rpkid_context, 311
irdb_query
rpki::rpki_engine::rpkid_context, 308
irdb_query_child_resources
rpki::rpki_engine::rpkid_context, 308
irdb_query_roa_requests
rpki::rpki_engine::rpkid_context, 308
irdb_url
rpki::rpki_engine::rpkid_context, 311
irdbd, 49
bpki_ta, 51
cfg, 51
cfg_ le, 51
client_ta, 51
cur, 51
db, 51
handle_dispatch, 51
handle_list_resources, 50
handle_list_roa_requests, 50
handler, 50
handlers, 52
host, 52
irdbd_cert, 52
irdbd_key, 52
port, 52
rpkid_cert, 52
server_cert, 52
startup_msg, 53
u, 53
irdbd.py(2913), 419
irdbd_cert
irdbd, 52
irdbd_key
irdbd, 52
is_CA
rpki::x509::DER_object, 375
is_cmd
irbe_cli::cmd_elt_mixin, 103
irbe_cli::reply_elt_mixin, 112

is_query
rpki::xml_utils::msg, 407
is_reply
rpki::xml_utils::msg, 407
is_set
rpki::async::timer, 131
issubset
rpki::resource_set::resource_set, 258
issue
rpki::rpki_engine::ca_detail_obj, 281
rpki::x509::X509, 393
issue_ee
rpki::rpki_engine::ca_detail_obj, 281
issue_subject_cert_maybe
rootd, 57
issuer
rpki::up_down::class_elt, 339
issuperset
rpki::resource_set::resource_set, 258
item_callback
rpki::async::iterator, 126
iterator
rpki::async::iterator, 126

key
rpki::https::http_client, 158
rpki::https::http_listener, 161
rpki::https::http_queue, 166

last_crl_sn
rpki::rpki_engine::ca_obj, 290
last_issued_sn
rpki::rpki_engine::ca_obj, 290
last_manifest_sn
rpki::rpki_engine::ca_obj, 290
lastrowid
rpki::sql::session, 314
later
rpki::sundial::datetime, 327
latest_ca_cert
rpki::rpki_engine::ca_detail_obj, 283
latest_crl
rpki::rpki_engine::ca_detail_obj, 283
latest_manifest
rpki::rpki_engine::ca_detail_obj, 284
latest_manifest_cert
rpki::rpki_engine::ca_detail_obj, 284
left_right
rpki::relaxng, 81
left_right.py(2931), 420
left_right_handler
rpki::rpki_engine::rpkid_context, 309
log
rpki::https::http_listener, 161
rpki::https::http_queue, 166
rpki::https::http_stream, 178
log.py(2933), 420
log_cert
rpki::https::http_stream, 177
log_method
rpki::https, 70
log_query
rootd::message_pdu, 121
rpki::up_down::message_pdu, 351
long, 114
looks_like_PEM
rpki::x509::PEM_converter, 378

maildir
rpki::x509::DeadDrop, 369
main
pubd, 54
rpkid, 94
make_b64elt
rpki::up_down::base_elt, 333
rpki::xml_utils::base_elt, 400
make_elt
rpki::up_down::base_elt, 334
rpki::xml_utils::base_elt, 400
make_pdu
rpki::xml_utils::base_elt, 400
make_pre x
rpki::resource_set::resource_range_ip, 254

make_publish
rpki::publication::publication_-object_elt, 240
make_query
rpki::up_down::message_pdu, 351
make_reply
rpki::left_right::list_published_-objects_elt, 196
rpki::xml_utils::data_elt, 403
make_reply_clone_hook
rpki::left_right::data_elt, 192
rpki::xml_utils::data_elt, 403
make_withdraw
rpki::publication::publication_-object_elt, 240
manifest.py(2424), 421
manifest_private_key_id
rpki::rpki_engine::ca_detail_obj, 284
manifest_public_key
rpki::rpki_engine::ca_detail_obj, 284
manifest_published
rpki::rpki_engine::ca_detail_obj, 284
manifest_published_callback
rpki::rpki_engine::ca_detail_obj, 281
manifest_uri
rpki::rpki_engine::ca_detail_obj, 281
manifestNumber
rpki::manifest::Manifest, 225
map
rpki::sql::template, 323
max
rpki::resource_set::resource_range, 251
rpki::resource_set::roa_pre x, 266
max_pre xlen
rpki::resource_set::roa_pre x, 267
maxLength
rpki::roa::ROAIPAddress, 273
min
rpki::resource_set::resource_range, 251
rpki::resource_set::resource_range_-as, 253
rpki::resource_set::roa_pre x, 266
msg
rpki::https::http_stream, 178
msgs
rpki::rpki_engine::publication_-queue, 297
multiget
rpki::con g::parser, 136

name
rpki::left_right::sax_handler, 213
rpki::publication::sax_handler, 246
rpki::up_down::sax_handler, 359
name2oid
rpki::oids, 79
name2type
rootd::message_pdu, 121
rpki::up_down::message_pdu, 352
next_crl_number
rpki::rpki_engine::ca_obj, 289
next_manifest_number
rpki::rpki_engine::ca_obj, 289
next_serial_number
rpki::rpki_engine::ca_obj, 289
nextUpdate
rpki::manifest::Manifest, 225
rpki::rpki_engine::ca_detail_obj, 284
normalize_chain
rpki::x509::X509, 394
normalize_headers
rpki::https::http_message, 163
note
rpki::log, 76
now
rpki::sundial, 88
nsmap
rpki::left_right::left_right_-namespace, 195
rpki::publication::publication_-namespace, 238
rpki::up_down, 90
obj

rpki::left_right::list_published_-
objects_elt, 196
object, 114
oid2name
rpki::oids, 79
oids.py(2424), 421
other_clear
rpki::x509::CMS_object, 363
rpki::x509::DER_object, 376
oversized
rpki::resource_set::resource_bag,
248

parent
rpki::rpki_engine::ca_obj, 289
parent_id
rpki::rpki_engine::ca_obj, 290
parent_resource_class
rpki::rpki_engine::ca_obj, 291
parents
rpki::left_right::bsc_elt, 183
rpki::left_right::child_elt, 187
rpki::left_right::repository_elt, 211
rpki::left_right::self_elt, 215
parse
rpki::sundial::timedelta, 332
parse_ rst_line
rpki::https::http_request, 168
rpki::https::http_response, 170
parse_from_wire
rpki::https::http_message, 163
parse_rfc3779_tuple
rpki::resource_set::resource_set_as,
260
rpki::resource_set::resource_set_ip,
262
parse_str
rpki::resource_set::resource_set_as,
260
rpki::resource_set::resource_set_ip,
262
rpki::resource_set::roa_pre x_set,
270
parse_type
rpki::https::http_client, 158
rpki::https::http_server, 172
parse_version
rpki::https::http_message, 163
password
rpki::sql::session, 316
path
rpki::https::http_request, 168
payload
rpki::publication::publication_-
object_elt, 241
rpki::up_down::message_pdu, 352
payload_type
rpki::publication::certi cate_elt, 226
rpki::publication::crl_elt, 235
rpki::publication::manifest_elt, 236
rpki::publication::publication_-
object_elt, 242
rpki::publication::roa_elt, 245
pdu
irbe_cli::left_right_sax_handler, 107
irbe_cli::publication_sax_handler,
110
rootd::sax_handler, 122
rpki::left_right::sax_handler, 213
rpki::publication::sax_handler, 246
rpki::up_down::sax_handler, 359
pdus
irbe_cli::left_right_msg, 106
irbe_cli::publication_msg, 110
rpki::left_right::msg, 202
rpki::publication::msg, 237
pem_converter
rpki::x509::CMS_object, 363
rpki::x509::CRL, 367
rpki::x509::DER_object, 377
rpki::x509::PKCS10, 381
rpki::x509::ROA, 383
rpki::x509::RSA, 385
rpki::x509::RSApublic, 388
rpki::x509::SignedManifest, 390
rpki::x509::X509, 394
pem_out
irbe_cli, 47
persistent
rpki::https::http_message, 163
pid
rpki::log, 77

rpki::x509::DeadDrop, 369
ping
rpki::sql::session, 315
pkcs10
rpki::up_down::issue_pdu, 347
pkcs10_request
rpki::left_right::bsc_elt, 185
PKIX_threshhold
rpki::sundial::datetime, 328
port
irdbd, 52
rootd, 59
POW
rpki::x509::CMS_object, 364
rpki::x509::CRL, 367
rpki::x509::RSA, 386
rpki::x509::RSApublic, 388
rpki::x509::X509, 395
POWify_OID
rpki::x509, 92
POWpkix
rpki::x509::CRL, 367
rpki::x509::PKCS10, 381
rpki::x509::X509, 395
pre x
rpki::resource_set::roa_pre x, 267
pre x_type
rpki::resource_set::roa_pre x_set_-
ipv4, 271
rpki::resource_set::roa_pre x_set_-
ipv6, 272
pre xlen
rpki::resource_set::roa_pre x, 267
pretty_print_content
rpki::x509::XML_CMS_object, 396
print_on_der_error
rpki::x509::CMS_object, 364
priority
rpki::log::logger, 222
private_key_id
rpki::left_right::bsc_elt, 185
rpki::rpki_engine::ca_detail_obj,
284
pro le
pubd, 54
rpkid, 94
pubd, 53
cfg_ le, 54
main, 54
pro le, 54
pubd.py(2913), 422
pubd::pubd_context, 114
__init__, 115
bpki_ta, 116
build_https_ta_cache, 115
clear_https_ta_cache, 115
client_handler, 116
client_url_regexp, 116
control_handler, 116
handler_common, 116
https_server_host, 117
https_server_port, 117
https_ta_cache, 117
irbe_cert, 117
pubd_cert, 117
pubd_key, 117
publication_base, 117
sql, 118
pubd_cert
pubd::pubd_context, 117
pubd_key
pubd::pubd_context, 117
public_key
rpki::rpki_engine::ca_detail_obj,
285
publication
rpki::relaxng, 81
publication.py(2935), 422
publication_base
pubd::pubd_context, 117
publication_kludge_base
rpki::rpki_engine::rpkid_context,
311
publish
rpki::rpki_engine::publication_-
queue, 296
published
rpki::rpki_engine::child_cert_obj,
294
rpki::rpki_engine::roa_obj, 305
published_callback

rpki::rpki_engine::child_cert_obj, 293
rpki::rpki_engine::roa_obj, 302
pydatetime::datetime, 118
pydatetime::timedelta, 118

q_msg
irbe_cli, 48
q_msg_left_right
irbe_cli, 48
q_msg_publication
irbe_cli, 48
q_pdu
irbe_cli, 48
query
rpki::up_down::issue_pdu, 346
rpki::up_down::list_pdu, 349
rpki::up_down::revoke_pdu, 355
rpki::xml_utils::msg, 407
query_up_down
rpki::left_right::parent_elt, 204
queue
rpki::async::timer, 133
rpki::https::http_client, 159
rpki::https::http_queue, 166

raise_if_error
rpki::publication::publication_-object_elt, 240
rpki::publication::report_error_elt, 243
range_type
rpki::resource_set::resource_set_as, 261
rpki::resource_set::resource_set_-ipv4, 263
rpki::resource_set::resource_set_-ipv6, 264
rpki::resource_set::roa_pre x_ipv4, 268
rpki::resource_set::roa_pre x_ipv6, 269
read_attrs
rpki::xml_utils::base_elt, 400
readable
rpki::https::http_stream, 177
reason
rpki::https::http_response, 170
recipient
rpki::up_down::message_pdu, 353
recv
rpki::https::http_stream, 177
regen_margin
rpki::left_right::self_elt, 220
regenerate
rpki::rpki_engine::roa_obj, 302
regenerate_crls_and_manifests
rpki::left_right::self_elt, 216
regexp
rpki::sundial::timedelta, 332
reissue
rpki::rpki_engine::child_cert_obj, 293
rekey
rpki::rpki_engine::ca_obj, 289
relaxng.py(2876), 423
replace
rpki::rpki_engine::publication_-queue, 297
reply
rpki::xml_utils::msg, 407
repositories
rpki::left_right::bsc_elt, 183
rpki::left_right::self_elt, 216
rpki::rpki_engine::publication_-queue, 297
repository
rpki::left_right::parent_elt, 204
req_resource_set_as
rpki::up_down::certi cate_elt, 336
rpki::up_down::issue_pdu, 347
req_resource_set_ipv4
rpki::up_down::certi cate_elt, 336
rpki::up_down::issue_pdu, 347
req_resource_set_ipv6
rpki::up_down::certi cate_elt, 336
rpki::up_down::issue_pdu, 347
request
rpki::https::http_queue, 165
require_crls
rpki::x509::CMS_object, 364
res

rpki::async::sync_wrapper, 128
resource_set.py(2776), 423
resource_set_as
rpki::up_down::class_elt, 339
resource_set_ipv4
rpki::up_down::class_elt, 339
resource_set_ipv6
rpki::up_down::class_elt, 339
resource_set_notafter
rpki::up_down::class_elt, 340
resource_set_type
rpki::resource_set::roa_pre x_set_ipv4, 271
rpki::resource_set::roa_pre x_set_ipv6, 272
restart
rpki::https::http_queue, 165
rpki::https::http_stream, 177
result
rpki::xml_utils::sax_handler, 411
retried
rpki::https::http_request, 169
retry_read
rpki::https::http_client, 159
rpki::https::http_server, 173
rpki::https::http_stream, 178
retry_write
rpki::https::http_client, 159
rpki::https::http_server, 173
rpki::https::http_stream, 178
return_result
rpki::https::http_queue, 165
revoke
rpki::rpki_engine::ca_detail_obj, 281
rpki::rpki_engine::ca_obj, 290
rpki::rpki_engine::child_cert_obj, 293
rpki::rpki_engine::revoked_cert_obj, 299
rpki::rpki_engine::roa_obj, 302
revoked
rpki::rpki_engine::revoked_cert_obj, 299
revoked_certs
rpki::rpki_engine::ca_detail_obj, 282
roa
rpki::rpki_engine::roa_obj, 305
roa.py(2424), 424
roas
rpki::left_right::self_elt, 216
rpki::rpki_engine::ca_detail_obj, 282
root_newer_than_subject
rootd, 58
rootd, 55
bpki_ta, 58
cfg, 58
cfg_ le, 58
child_bpki_cert, 59
client_ta, 59
compose_response, 57
del_subject_cert, 57
del_subject_pkcs10, 57
get_root_cert, 57
get_subject_cert, 57
get_subject_pkcs10, 57
handlers, 59
host, 59
https_server_host, 59
https_server_port, 59
issue_subject_cert_maybe, 57
port, 59
root_newer_than_subject, 58
rootd_bpki_cert, 60
rootd_bpki_crl, 60
rootd_bpki_key, 60
rpki_base_uri, 60
rpki_class_name, 60
rpki_root_cert, 60
rpki_root_cert_ le, 60
rpki_root_cert_uri, 61
rpki_root_crl, 61
rpki_root_dir, 61
rpki_root_key, 61
rpki_root_manifest, 61
rpki_subject_cert, 61
rpki_subject_lifetime, 61
rpki_subject_pkcs10, 62
rpki_subject_regen, 62

server_cert, 62
set_subject_cert, 58
set_subject_pkcs10, 58
up_down_handler, 58
rootd.py(2913), 425
rootd::cms_msg, 118
saxify, 119
rootd::issue_pdu, 119
serve_pdu, 119
rootd::list_pdu, 119
serve_pdu, 120
rootd::message_pdu, 120
log_query, 121
name2type, 121
type2name, 121
rootd::revoke_pdu, 121
serve_pdu, 122
rootd::sax_handler, 122
pdu, 122
rootd_bpki_cert
rootd, 60
rootd_bpki_crl
rootd, 60
rootd_bpki_key
rootd, 60
rpki, 62
rpki.async, 63
rpki.con g, 65
rpki.exceptions, 66
rpki.https, 68
rpki.ipaddrs, 72
rpki.left_right, 73
rpki.log, 74
rpki.manifest, 77
rpki.oids, 78
rpki.publication, 80
rpki.relaxng, 81
rpki.resource_set, 81
rpki.roa, 84
rpki.rpki_engine, 85
rpki.sql, 86
rpki.sundial, 87
rpki.up_down, 89
rpki.x509, 90
rpki.xml_utils, 92
rpki::async
_raiseExitNow, 64
defer, 64
deferred_queue, 65
event_loop, 64
exit_event_loop, 64
ExitNow, 65
run_deferred, 64
rpki::async::gc_summary, 123
__init__, 123
handler, 123
interval, 124
timer, 124
rpki::async::iterator, 124
__call__, 125
__init__, 125
__repr__, 125
caller_function, 126
doit, 125
done_callback, 126
ignore, 125
item_callback, 126
iterator, 126
unwind_stack, 126
rpki::async::sync_wrapper, 126
__call__, 127
__init__, 127
cb, 127
eb, 127
err, 128
func, 128
res, 128
rpki::async::timer, 128
__cmp__, 130
__del__, 130
__init__, 130
__repr__, 130
cancel, 130
clear, 130
errback, 130, 132
gc_debug, 132
handler, 131, 133
is_set, 131
queue, 133
run_debug, 133
runq, 131
seconds_until_wakeup, 131

set, 131
set_errback, 132
set_handler, 132
trace, 132
when, 133
rpki::con g::parser, 133
__init__, 134
_get_wrapper, 134
cfg, 136
default_section, 136
lename, 136
get, 135
getboolean, 135
getint, 135
has_option, 135
has_section, 135
multiget, 136
set_global_ ags, 136
rpki::exceptions::BadClassNameSyntax, 137
rpki::exceptions::BadClientURL, 137
rpki::exceptions::BadContactURL, 137
rpki::exceptions::BadExtension, 138
rpki::exceptions::BadIRDBReply, 138
rpki::exceptions::BadIssueResponse, 138
rpki::exceptions::BadPKCS10, 139
rpki::exceptions::BadPublicationReply, 139
rpki::exceptions::BadQuery, 139
rpki::exceptions::BadSender, 140
rpki::exceptions::BadStatusCode, 140
rpki::exceptions::BadURISyntax, 140
rpki::exceptions::BSCNotFound, 141
rpki::exceptions::BSCNotReady, 141
rpki::exceptions::ChildNotFound, 141
rpki::exceptions::ClassNameMismatch, 142
rpki::exceptions::ClassNameUnknown, 142
rpki::exceptions::ClientNotFound, 142
rpki::exceptions::CMSContentNotSet, 143
rpki::exceptions::CMSCRLNotSet, 143
rpki::exceptions::CMSVeri cationFailed, 143
rpki::exceptions::DBConsistancyError, 144
rpki::exceptions::DERObjectConversionError, 144
rpki::exceptions::DuplicateObject, 144
rpki::exceptions::EmptyPEM, 145
rpki::exceptions::EmptyROAPre xList, 145
rpki::exceptions::ForbiddenURL, 145
rpki::exceptions::HandleTranslationError, 146
rpki::exceptions::HTTPRequestFailed, 146
rpki::exceptions::HTTPSBadVersion, 146
rpki::exceptions::HTTPSClientAborted, 147
rpki::exceptions::HTTPSUnexpectedState, 147
rpki::exceptions::MissingCMSCRL, 147
rpki::exceptions::MissingCMSEEcert, 148
rpki::exceptions::MultipleTLSEECert, 148
rpki::exceptions::MustBePre x, 148
rpki::exceptions::NoActiveCA, 149
rpki::exceptions::NoCoveringCertForROA, 149
rpki::exceptions::NoObjectAtURI, 149
rpki::exceptions::NotACerti cateChain, 150
rpki::exceptions::NotFound, 150
rpki::exceptions::NotImplementedYet, 150
rpki::exceptions::NotInDatabase, 151
rpki::exceptions::ReceivedTLSCACert, 151
rpki::exceptions::RPKI_Exception, 151
rpki::exceptions::ServerShuttingDown, 152
rpki::exceptions::SKIMismatch, 153
rpki::exceptions::SubprocessError, 153
rpki::exceptions::TLSValidationError, 153
rpki::exceptions::UnexpectedCMSCerts, 154

rpki::exceptions::UnexpectedCMSCRLs, 154
rpki::exceptions::UnparsableCMSDER, 154
rpki::exceptions::UpstreamError, 155
rpki::exceptions::WrongEContentType, 155
rpki::https
build_https_ta_cache, 69
client, 70
client_queues, 70
debug_http, 70
debug_tls_certs, 70
default_client_timeout, 71
default_http_version, 71
default_server_timeout, 71
log_method, 70
rpki_content_type, 71
server, 70
want_persistent_client, 71
want_persistent_server, 71
rpki::https::http_client, 155
__init__, 156
cert, 158
expect_close, 158
handle_close, 156
handle_connect, 157
handle_error, 157
handle_message, 157
handle_no_content_length, 157
handle_timeout, 157
hostport, 158
key, 158
parse_type, 158
queue, 159
retry_read, 159
retry_write, 159
send_request, 157
set_state, 157
start, 158
state, 159
ta, 159
timeout, 159
tls, 159
tls_connect, 158
rpki::https::http_listener, 160
__init__, 160
cert, 161
dynamic_ta, 161
handle_accept, 161
handle_error, 161
handlers, 161
key, 161
log, 161
ta, 161
rpki::https::http_message, 162
__init__, 163
__str__, 163
body, 164
format, 163
headers, 164
normalize_headers, 163
parse_from_wire, 163
parse_version, 163
persistent, 163
software_name, 164
version, 164
rpki::https::http_queue, 164
__init__, 165
cert, 166
client, 166
detach, 165
hostport, 166
key, 166
log, 166
queue, 166
request, 165
restart, 165
return_result, 165
send_request, 166
ta, 167
rpki::https::http_request, 167
__init__, 168
callback, 168
cmd, 168
errback, 168
format_ rst_line, 168
parse_ rst_line, 168
path, 168
retried, 169
rpki::https::http_response, 169
__init__, 169

code,170
format_ rst_line,169
parse_ rst_line,170
reason,170
rpki::https::http_server,170
__init__,171
expect_close,172
nd_handler,171
handle_message,171
handle_no_content_length,171
handlers,172
parse_type,172
retry_read,173
retry_write,173
send_error,172
send_message,172
send_reply,172
timeout,173
tls, 173
tls_accept,172
rpki::https::http_stream,173
__init__,175
buffer, 178
chunk_body,175
chunk_discard_crlf,175
chunk_discard_trailer,175
chunk_handler,178
chunk_header,175
close,175
collect_incoming_data,175
found_terminator,175
get_buffer,176
handle_body,176
handle_close,176
handle_error,176
handle_read,176
handle_timeout,176
handle_write,176
initiate_send,177
log, 178
log_cert,177
msg,178
readable,177
recv,177
restart,177
retry_read,178
retry_write,178
send,177
timer, 179
tls, 179
update_timeout,177
writeable,178
rpki::ipaddrs::v4addr,179
__new__,180
__str__,180
bits, 180
from_bytes,180
to_bytes,180
rpki::ipaddrs::v6addr,181
__new__,181
__str__,181
bits, 182
from_bytes,181
to_bytes,182
rpki::left_right
enforce_strict_up_down_xml_-
sender,74
rpki::left_right::bsc_elt,182
attributes,184
booleans,184
children,183
element_name,184
elements,185
handles,185
parents,183
pkcs10_request,185
private_key_id,185
repositories,183
serve_pre_save_hook,184
signing_cert,185
signing_cert_crl,185
sql_template,186
rpki::left_right::child_elt,186
attributes,188
booleans,188
bpki_cert,189
bpki_glue,189
ca_from_class_name,187
child_certs,187
clear_https_ta_cache,189
element_name,189
elements,189

endElement, 187
handles, 189
parents, 187
serve_destroy_hook, 188
serve_post_save_hook, 188
serve_up_down, 188
sql_template, 190
rpki::left_right::cms_msg, 190
encoding, 191
saxify, 191
schema, 191
rpki::left_right::data_elt, 191
bsc, 192
handles, 194
make_reply_clone_hook, 192
self, 192
self_handle, 194
self_id, 194
serve_fetch_all, 192
serve_fetch_handle, 193
serve_fetch_one_maybe, 193
serve_pre_save_hook, 193
rpki::left_right::left_right_namespace, 194
nsmap, 195
xmlns, 195
rpki::left_right::list_published_objects_elt, 195
attributes, 196
element_name, 196
make_reply, 196
obj, 196
serve_dispatch, 196
text_attribute, 197
rpki::left_right::list_resources_elt, 197
asn, 198
attributes, 198
element_name, 199
ipv4, 199
ipv6, 199
startElement, 198
toXML, 198
valid_until, 199
rpki::left_right::list_roa_requests_elt, 199
attributes, 200
element_name, 200
ipv4, 201
ipv6, 201
startElement, 200
rpki::left_right::msg, 201
pdus, 202
serve_top_level, 202
version, 202
rpki::left_right::parent_elt, 203
attributes, 205
booleans, 205
bpki_cms_cert, 205
bpki_cms_glue, 206
bpki_https_cert, 206
bpki_https_glue, 206
cas, 204
element_name, 206
elements, 206
handles, 206
query_up_down, 204
repository, 204
serve_post_save_hook, 204
serve_rekey, 204
serve_revoke, 204
serve_revoke_forgotten, 205
sql_template, 207
rpki::left_right::report_error_elt, 207
attributes, 208
element_name, 208
error_code, 209
error_text, 209
from_exception, 208
self_handle, 209
tag, 209
text_attribute, 209
rpki::left_right::repository_elt, 209
attributes, 211
bpki_cert, 211
bpki_glue, 211
call_pubd, 210
default_pubd_handle, 210
element_name, 211
elements, 212
handles, 212
parents, 211
sql_template, 212
rpki::left_right::sax_handler, 212

name, 213
pdu, 213
version, 213
rpki::left_right::self_elt, 213
attributes, 219
booleans, 219
bpki_cert, 219
bpki_glue, 219
bscs, 215
children, 215
client_poll, 215
crl_interval, 220
cron, 215
element_name, 220
elements, 220
handles, 220
parents, 215
regen_margin, 220
regenerate_crls_and_manifests, 216
repositories, 216
roas, 216
serve_fetch_all, 216
serve_fetch_handle, 217
serve_fetch_one_maybe, 217
serve_post_save_hook, 217
serve_publish_world_now, 217
serve_rekey, 218
serve_revoke, 218
serve_revoke_forgotten, 218
serve_run_now, 218
sql_template, 220
update_children, 218
update_roas, 219
use_hsm, 221
rpki::log
debug, 76
enable_trace, 76
error, 76
info, 76
init, 75
note, 76
pid, 77
set_trace, 75
tag, 77
trace, 75
traceback, 76
use_syslog, 77
warn, 77
rpki::log::logger, 221
__call__, 221
__init__, 221
priority, 222
rpki::manifest::FileAndHash, 222
__init__, 222
le, 223
hash, 223
rpki::manifest::FilesAndHashes, 223
__init__, 223
rpki::manifest::Manifest, 224
__init__, 224
explicitVersion, 224
leHashAlg, 224
leList, 224
manifestNumber, 225
nextUpdate, 225
thisUpdate, 225
version, 225
rpki::oids
name2oid, 79
oid2name, 79
rpki::publication::certi cate_elt, 225
element_name, 226
payload_type, 226
rpki::publication::client_elt, 226
attributes, 228
base_uri, 228
bpki_cert, 228
bpki_glue, 229
check_allowed_uri, 227
clear_https_ta_cache, 229
element_name, 229
elements, 229
endElement, 227
serve_fetch_all, 227
serve_fetch_one_maybe, 228
serve_post_save_hook, 228
sql_template, 229
rpki::publication::cms_msg, 230
encoding, 230
saxify, 230
schema, 230
rpki::publication::con g_elt, 231

attributes, 233
con g_id, 233
element_name, 233
elements, 233
fetch, 232
serve_fetch_one_maybe, 232
serve_set, 232
sql_template, 233
startElement, 232
wired_in_con g_id, 233
rpki::publication::control_elt, 234
serve_dispatch, 234
rpki::publication::crl_elt, 235
element_name, 235
payload_type, 235
rpki::publication::manifest_elt, 235
element_name, 236
payload_type, 236
rpki::publication::msg, 236
pdus, 237
serve_top_level, 237
version, 237
rpki::publication::publication_-namespace, 238
nsmap, 238
xmlns, 238
rpki::publication::publication_object_elt, 239
attributes, 241
endElement, 240
make_publish, 240
make_withdraw, 240
payload, 241
payload_type, 242
raise_if_error, 240
serve_dispatch, 240
serve_publish, 240
serve_withdraw, 241
toXML, 241
uri_to_ lename, 241
rpki::publication::report_error_elt, 242
__str__, 243
attributes, 243
element_name, 244
error_code, 244
error_text, 244
from_exception, 243
raise_if_error, 243
tag, 244
text_attribute, 244
rpki::publication::roa_elt, 245
element_name, 245
payload_type, 245
rpki::publication::sax_handler, 245
name, 246
pdu, 246
version, 246
rpki::relaxng
left_right, 81
publication, 81
up_down, 81
rpki::resource_set
_bs2long, 83
_long2bs, 83
_rsplit, 83
inherit_token, 84
test1, 84
test2, 84
rpki::resource_set::resource_bag, 246
__eq__, 247
__init__, 247
__ne__, 248
__str__, 248
asn, 249
empty, 248
from_rfc3779_tuples, 248
intersection, 248
oversized, 248
undersized, 249
union, 249
v4, 249
v6, 249
valid_until, 250
rpki::resource_set::resource_range, 250
__cmp__, 251
__init__, 251
max, 251
min, 251
rpki::resource_set::resource_range_as, 251
__str__, 252
datum_type, 252

min, 253
to_rfc3779_tuple, 252
rpki::resource_set::resource_range_ip, 253
__str__, 254
_pre xlen, 254
make_pre x, 254
to_rfc3779_tuple, 254
rpki::resource_set::resource_range_ipv4, 254
datum_type, 255
rpki::resource_set::resource_range_ipv6, 255
datum_type, 256
rpki::resource_set::resource_set, 256
__init__, 257
__str__, 257
_comm, 257
contains, 257
difference, 257
from_sql, 258
inherit, 259
intersection, 258
issubset, 258
issuperset, 258
symmetric_difference, 258
union, 259
rpki::resource_set::resource_set_as, 259
inherit, 261
parse_rfc3779_tuple, 260
parse_str, 260
range_type, 261
to_rfc3779_tuple, 260
rpki::resource_set::resource_set_ip, 261
inherit, 262
parse_rfc3779_tuple, 262
parse_str, 262
to_rfc3779_tuple, 262
rpki::resource_set::resource_set_ipv4, 263
a , 263
range_type, 263
rpki::resource_set::resource_set_ipv6, 264
a , 264
range_type, 264
rpki::resource_set::roa_pre x, 265
__cmp__, 265
__init__, 266
__str__, 266
max, 266
max_pre xlen, 267
min, 266
pre x, 267
pre xlen, 267
to_resource_range, 266
to_roa_tuple, 267
rpki::resource_set::roa_pre x_ipv4, 267
range_type, 268
rpki::resource_set::roa_pre x_ipv6, 268
range_type, 269
rpki::resource_set::roa_pre x_set, 269
__init__, 269
__str__, 269
from_sql, 270
parse_str, 270
to_resource_set, 270
to_roa_tuple, 270
rpki::resource_set::roa_pre x_set_ipv4, 271
pre x_type, 271
resource_set_type, 271
rpki::resource_set::roa_pre x_set_ipv6, 272
pre x_type, 272
resource_set_type, 272
rpki::roa::ROAIPAddress, 273
__init__, 273
address, 273
maxLength, 273
rpki::roa::ROAIPAddresses, 274
__init__, 274
rpki::roa::ROAIPAddressFamilies, 274
__init__, 275
rpki::roa::ROAIPAddressFamily, 275
__init__, 275
addresses, 276
addressFamily, 276
rpki::roa::RouteOriginAttestation, 276
__init__, 276
asID, 277
explicitVersion, 277

ipAddrBlocks, 277
version, 277
rpki::rpki_engine::ca_detail_obj, 277
activate, 279
ca, 279
ca_cert_uri, 283
ca_id, 283
child_certs, 279
create, 279
crl_published, 283
crl_published_callback, 279
crl_uri, 279
crl_uri_tail, 280
delete, 280
gctx, 283
generate_crl, 280
generate_manifest, 280
generate_manifest_cert, 280
issue, 281
issue_ee, 281
latest_ca_cert, 283
latest_crl, 283
latest_manifest, 284
latest_manifest_cert, 284
manifest_private_key_id, 284
manifest_public_key, 284
manifest_published, 284
manifest_published_callback, 281
manifest_uri, 281
nextUpdate, 284
private_key_id, 284
public_key, 285
revoke, 281
revoked_certs, 282
roas, 282
sql_decode, 282
sql_template, 285
state, 285
update, 282
rpki::rpki_engine::ca_obj, 285
ca_details, 287
check_for_updates, 287
construct_sia_uri, 287
create, 287
delete, 287
fetch_active, 288
fetch_deprecated, 288
fetch_issue_response_candidates, 288
fetch_pending, 288
fetch_revoked, 288
gctx, 290
last_crl_sn, 290
last_issued_sn, 290
last_manifest_sn, 290
next_crl_number, 289
next_manifest_number, 289
next_serial_number, 289
parent, 289
parent_id, 290
parent_resource_class, 291
rekey, 289
revoke, 290
sia_uri, 291
sql_template, 291
rpki::rpki_engine::child_cert_obj, 291
__init__, 292
ca_detail, 292
ca_detail_id, 294
cert, 294
child, 292
child_id, 294
fetch, 293
gctx, 294
published, 294
published_callback, 293
reissue, 293
revoke, 293
sql_template, 295
uri, 293
uri_tail, 294
rpki::rpki_engine::publication_queue, 295
__init__, 296
_add, 296
call_pubd, 296
handlers, 297
msgs, 297
publish, 296
replace, 297
repositories, 297
uris, 297

withdraw, 296
rpki::rpki_engine::revoked_cert_obj, 298
__init__, 298
ca_detail, 298
ca_detail_id, 299
expires, 299
gctx, 299
revoke, 299
revoked, 299
serial, 299
sql_template, 300
rpki::rpki_engine::roa_obj, 300
__init__, 301
asn, 304
ca_detail, 301
ca_detail_id, 304
cert, 304
gctx, 304
generate, 301
ipv4, 305
ipv6, 305
published, 305
published_callback, 302
regenerate, 302
revoke, 302
roa, 305
self, 303
self_id, 305
sql_delete_hook, 303
sql_fetch_hook, 303
sql_insert_hook, 303
sql_template, 305
update, 303
uri, 304
uri_tail, 304
rpki::rpki_engine::rpkid_context, 306
__init__, 307
bpki_ta, 309
build_https_ta_cache, 307
checkpoint, 307
clear_https_ta_cache, 307
cron, 308
cron_keepalive, 309
cron_period, 310
cron_timeout, 310
cron_timer, 310
cronjob_handler, 308
https_server_host, 310
https_server_port, 310
https_ta_cache, 310
initial_delay, 310
irbe_cert, 311
irdb_cert, 311
irdb_query, 308
irdb_query_child_resources, 308
irdb_query_roa_requests, 308
irdb_url, 311
left_right_handler, 309
publication_kludge_base, 311
rpkid_cert, 311
rpkid_key, 311
sql, 311
start_cron, 309
up_down_handler, 309
up_down_url_regexp, 312
use_internal_cron, 312
rpki::sql::session, 312
__init__, 313
_exceptions_enabled, 315
_wrap_execute, 313
assert_pristine, 313
cache, 315
cache_clear, 314
close, 314
connect, 314
cur, 315
database, 315
db, 316
dirty, 316
execute, 314
executemany, 314
fetchall, 314
lastrowid, 314
password, 316
ping, 315
sweep, 315
username, 316
rpki::sql::sql_persistent, 316
gctx, 321
sql_debug, 321
sql_decode, 317
sql_delete, 318

sql_delete_hook, 318
sql_deleted, 321
sql_encode, 318
sql_fetch, 318
sql_fetch_all, 319
sql_fetch_hook, 319
sql_fetch_where, 319
sql_fetch_where1, 319
sql_in_db, 322
sql_init, 319
sql_insert_hook, 320
sql_is_dirty, 320
sql_mark_clean, 320
sql_mark_deleted, 320
sql_mark_dirty, 320
sql_store, 321
sql_update_hook, 321
rpki::sql::template, 322
__init__, 323
columns, 323
delete, 323
index, 323
insert, 323
map, 323
select, 323
table, 324
update, 324
rpki::sundial
_cast, 88
now, 88
test, 88
rpki::sundial::datetime, 324
__add__, 325
__radd__, 325
__rsub__, 325
__str__, 325
__sub__, 325
earlier, 326
from_sql, 326
fromASN1tuple, 326
fromdatetime, 326
fromGeneralizedTime, 326
fromUTCTime, 326
fromXMLtime, 327
later, 327
PKIX_threshhold, 328
to_sql, 327
toASN1tuple, 327
toGeneralizedTime, 327
totimestamp, 328
toUTCTime, 328
toXMLtime, 328
rpki::sundial::timedelta, 329
__abs__, 330
__add__, 330
__div__, 330
__ oordiv__, 330
__mul__, 330
__neg__, 330
__pos__, 330
__radd__, 330
__rdiv__, 331
__r oordiv__, 331
__rmul__, 331
__rsub__, 331
__sub__, 331
convert_to_seconds, 331
fromtimedelta, 331
parse, 332
regexp, 332
rpki::up_down
nsmap, 90
xmlns, 90
rpki::up_down::base_elt, 332
check_response, 333
endElement, 333
make_b64elt, 333
make_elt, 334
serve_pdu, 334
startElement, 334
rpki::up_down::certi cate_elt, 335
cert, 336
cert_url, 336
endElement, 335
req_resource_set_as, 336
req_resource_set_ipv4, 336
req_resource_set_ipv6, 336
startElement, 335
toXML, 336
rpki::up_down::class_elt, 337
__init__, 338
cert_url, 339

certs, 339
class_name, 339
endElement, 338
from_resource_bag, 338
issuer, 339
resource_set_as, 339
resource_set_ipv4, 339
resource_set_ipv6, 339
resource_set_notafter, 340
startElement, 338
suggested_sia_head, 340
to_resource_bag, 338
toXML, 338
rpki::up_down::class_response_syntax, 340
__init__, 341
classes, 341
startElement, 341
toXML, 341
rpki::up_down::cms_msg, 341
encoding, 342
saxify, 342
schema, 342
rpki::up_down::error_response_pdu, 342
__init__, 343
check_response, 343
codes, 344
description, 344
endElement, 343
exceptions, 344
status, 345
toXML, 344
rpki::up_down::issue_pdu, 345
class_name, 347
endElement, 346
pkcs10, 347
query, 346
req_resource_set_as, 347
req_resource_set_ipv4, 347
req_resource_set_ipv6, 347
serve_pdu, 346
startElement, 346
toXML, 346
rpki::up_down::issue_response_pdu, 348
check_response, 348
rpki::up_down::list_pdu, 348
query, 349
serve_pdu, 349
toXML, 349
rpki::up_down::list_response_pdu, 349
rpki::up_down::message_pdu, 350
__str__, 351
log_query, 351
make_query, 351
name2type, 352
payload, 352
recipient, 353
sender, 353
serve_error, 351
serve_top_level, 351
startElement, 352
toXML, 352
type, 353
type2name, 353
version, 353
rpki::up_down::multi_uri, 354
__init__, 354
__str__, 354
rsync, 354
rpki::up_down::revoke_pdu, 355
class_name, 356
get_SKI, 355
query, 355
serve_pdu, 356
ski, 356
rpki::up_down::revoke_response_pdu, 356
rpki::up_down::revoke_syntax, 357
class_name, 358
ski, 358
startElement, 357
toXML, 357
rpki::up_down::sax_handler, 358
name, 359
pdu, 359
version, 359
rpki::x509
calculate_SKI, 92
POWify_OID, 92
rpki::x509::CMS_object, 359
content, 362
debug_cms_certs, 362

DER, 362
dump_on_verify_failure, 363
econtent_oid, 363
extract, 361
formats, 363
get_content, 361
get_DER, 361
get_POW, 361
other_clear, 363
pem_converter, 363
POW, 364
print_on_der_error, 364
require_crls, 364
set_content, 361
sign, 362
verify, 362
rpki::x509::CRL, 364
DER, 367
formats, 367
generate, 365
get_DER, 365
get_POW, 366
get_POWpkix, 366
getIssuer, 366
getNextUpdate, 366
getThisUpdate, 366
pem_converter, 367
POW, 367
POWpkix, 367
rpki::x509::DeadDrop, 368
__init__, 368
dump, 368
maildir, 369
pid, 369
rpki::x509::DER_CMS_object, 369
content, 370
decode, 370
encode, 370
rpki::x509::DER_object, 370
__cmp__, 372
__init__, 372
clear, 372
DER, 376
dumpasn1, 372
empty, 372
formats, 376
from_sql, 372
gAKI, 373
get_3779resources, 373
get_AIA, 373
get_AKI, 373
get_Base64, 373
get_basicConstraints, 374
get_DER, 374
get_PEM, 374
get_SIA, 374
get_SKI, 374
gSKI, 375
hAKI, 375
hSKI, 375
is_CA, 375
other_clear, 376
pem_converter, 377
set, 375
to_sql, 376
rpki::x509::PEM_converter, 377
__init__, 378
b, 378
e, 378
looks_like_PEM, 378
to_DER, 378
to_PEM, 378
rpki::x509::PKCS10, 379
check_valid_rpki, 380
create, 380
create_ca, 380
DER, 381
formats, 381
get_DER, 380
get_POWpkix, 380
getPublicKey, 380
pem_converter, 381
POWpkix, 381
rpki::x509::ROA, 382
build, 382
content_class, 382
econtent_oid, 382
pem_converter, 383
rpki::x509::RSA, 383
DER, 385
formats, 385
generate, 384

get_DER, 384
get_POW, 384
get_public_DER, 384
get_RSApublic, 385
get_SKI, 385
pem_converter, 385
POW, 386
rpki::x509::RSApublic, 386
DER, 387
formats, 388
get_DER, 387
get_POW, 387
get_SKI, 387
pem_converter, 388
POW, 388
rpki::x509::SignedManifest, 388
build, 389
content_class, 390
econtent_oid, 390
getNextUpdate, 389
getThisUpdate, 389
pem_converter, 390
rpki::x509::X509, 390
cross_certify, 391
DER, 394
expired, 392
formats, 394
get_DER, 392
get_POW, 392
get_POWpkix, 392
getIssuer, 392
getNotAfter, 392
getNotBefore, 393
getPublicKey, 393
getSerial, 393
getSubject, 393
issue, 393
normalize_chain, 394
pem_converter, 394
POW, 395
POWpkix, 395
rpki::x509::XML_CMS_object, 395
content, 397
decode, 396
dump_inbound_cms, 397
dump_outbound_cms, 398
dump_to_disk, 396
econtent_oid, 398
encode, 396
pretty_print_content, 396
schema_check, 397
unwrap, 397
wrap, 397
rpki::xml_utils::base_elt, 398
__str__, 399
attributes, 401
booleans, 401
elements, 401
endElement, 399
make_b64elt, 400
make_elt, 400
make_pdu, 400
read_attrs, 400
startElement, 400
toXML, 401
rpki::xml_utils::data_elt, 402
endElement, 403
make_reply, 403
make_reply_clone_hook, 403
serve_create, 403
serve_destroy, 403
serve_destroy_hook, 403
serve_dispatch, 404
serve_fetch_one, 404
serve_get, 404
serve_list, 404
serve_post_save_hook, 404
serve_pre_save_hook, 405
serve_set, 405
toXML, 405
unimplemented_control, 405
rpki::xml_utils::msg, 406
__str__, 407
endElement, 407
is_query, 407
is_reply, 407
query, 407
reply, 407
startElement, 408
toXML, 408
type, 408
version, 408

rpki::xml_utils::sax_handler, 409
__init__, 409
characters, 410
create_top_level, 410
endElement, 410
endElementNS, 410
result, 411
saxify, 410
stack, 411
startElement, 410
startElementNS, 411
text, 411
rpki::xml_utils::text_elt, 412
endElement, 412
text_attribute, 413
toXML, 412
rpki_base_uri
rootd, 60
rpki_class_name
rootd, 60
rpki_content_type
rpki::https, 71
rpki_engine.py(2934), 426
rpki_root_cert
rootd, 60
rpki_root_cert_ le
rootd, 60
rpki_root_cert_uri
rootd, 61
rpki_root_crl
rootd, 61
rpki_root_dir
rootd, 61
rpki_root_key
rootd, 61
rpki_root_manifest
rootd, 61
rpki_subject_cert
rootd, 61
rpki_subject_lifetime
rootd, 61
rpki_subject_pkcs10
rootd, 62
rpki_subject_regen
rootd, 62
rpkid, 93
cfg_ le, 94
main, 94
pro le, 94
rpkid.py(2913), 427
rpkid_cert
irdbd, 52
rpki::rpki_engine::rpkid_context, 311
rpkid_key
rpki::rpki_engine::rpkid_context, 311
rsync
rpki::up_down::multi_uri, 354
run_debug
rpki::async::timer, 133
run_deferred
rpki::async, 64
runq
rpki::async::timer, 131

saxify
irbe_cli::left_right_cms_msg, 106
irbe_cli::publication_cms_msg, 109
rootd::cms_msg, 119
rpki::left_right::cms_msg, 191
rpki::publication::cms_msg, 230
rpki::up_down::cms_msg, 342
rpki::xml_utils::sax_handler, 410
schema
rpki::left_right::cms_msg, 191
rpki::publication::cms_msg, 230
rpki::up_down::cms_msg, 342
schema_check
rpki::x509::XML_CMS_object, 397
seconds_until_wakeup
rpki::async::timer, 131
select
rpki::sql::template, 323
self
rpki::left_right::data_elt, 192
rpki::rpki_engine::roa_obj, 303
self_handle
rpki::left_right::data_elt, 194
rpki::left_right::report_error_elt, 209
self_id
rpki::left_right::data_elt, 194

rpki::rpki_engine::roa_obj, 305
send
rpki::https::http_stream, 177
send_error
rpki::https::http_server, 172
send_message
rpki::https::http_server, 172
send_reply
rpki::https::http_server, 172
send_request
rpki::https::http_client, 157
rpki::https::http_queue, 166
sender
rpki::up_down::message_pdu, 353
Sequence, 413
SequenceOf, 413
serial
rpki::rpki_engine::revoked_cert_obj, 299
serve_create
rpki::xml_utils::data_elt, 403
serve_destroy
rpki::xml_utils::data_elt, 403
serve_destroy_hook
rpki::left_right::child_elt, 188
rpki::xml_utils::data_elt, 403
serve_dispatch
rpki::left_right::list_published_objects_elt, 196
rpki::publication::control_elt, 234
rpki::publication::publication_object_elt, 240
rpki::xml_utils::data_elt, 404
serve_error
rpki::up_down::message_pdu, 351
serve_fetch_all
rpki::left_right::data_elt, 192
rpki::left_right::self_elt, 216
rpki::publication::client_elt, 227
serve_fetch_handle
rpki::left_right::data_elt, 193
rpki::left_right::self_elt, 217
serve_fetch_one
rpki::xml_utils::data_elt, 404
serve_fetch_one_maybe
rpki::left_right::data_elt, 193
rpki::left_right::self_elt, 217
rpki::publication::client_elt, 228
rpki::publication::con g_elt, 232
serve_get
rpki::xml_utils::data_elt, 404
serve_list
rpki::xml_utils::data_elt, 404
serve_pdu
rootd::issue_pdu, 119
rootd::list_pdu, 120
rootd::revoke_pdu, 122
rpki::up_down::base_elt, 334
rpki::up_down::issue_pdu, 346
rpki::up_down::list_pdu, 349
rpki::up_down::revoke_pdu, 356
serve_post_save_hook
rpki::left_right::child_elt, 188
rpki::left_right::parent_elt, 204
rpki::left_right::self_elt, 217
rpki::publication::client_elt, 228
rpki::xml_utils::data_elt, 404
serve_pre_save_hook
rpki::left_right::bsc_elt, 184
rpki::left_right::data_elt, 193
rpki::xml_utils::data_elt, 405
serve_publish
rpki::publication::publication_object_elt, 240
serve_publish_world_now
rpki::left_right::self_elt, 217
serve_rekey
rpki::left_right::parent_elt, 204
rpki::left_right::self_elt, 218
serve_revoke
rpki::left_right::parent_elt, 204
rpki::left_right::self_elt, 218
serve_revoke_forgotten
rpki::left_right::parent_elt, 205
rpki::left_right::self_elt, 218
serve_run_now
rpki::left_right::self_elt, 218
serve_set
rpki::publication::con g_elt, 232
rpki::xml_utils::data_elt, 405
serve_top_level
rpki::left_right::msg, 202

rpki::publication::msg, 237
rpki::up_down::message_pdu, 351
serve_up_down
rpki::left_right::child_elt, 188
serve_withdraw
rpki::publication::publication_object_elt, 241
server
rpki::https, 70
server_cert
irbe_cli::caller, 98
irdbd, 52
rootd, 62
server_ta
irbe_cli::caller, 98
set
rpki::async::timer, 131
rpki::x509::DER_object, 375
set_content
rpki::x509::CMS_object, 361
set_errback
rpki::async::timer, 132
set_global_ ags
rpki::con g::parser, 136
set_handler
rpki::async::timer, 132
set_state
rpki::https::http_client, 157
set_subject_cert
rootd, 58
set_subject_pkcs10
rootd, 58
set_trace
rpki::log, 75
sia_uri
rpki::rpki_engine::ca_obj, 291
sign
rpki::x509::CMS_object, 362
signing_cert
irbe_cli::bsc_elt, 97
rpki::left_right::bsc_elt, 185
signing_cert_crl
irbe_cli::bsc_elt, 97
rpki::left_right::bsc_elt, 185
ski
rpki::up_down::revoke_pdu, 356
rpki::up_down::revoke_syntax, 358
software_name
rpki::https::http_message, 164
sql
pubd::pubd_context, 118
rpki::rpki_engine::rpkid_context, 311
sql.py(2895), 427
sql_debug
rpki::sql::sql_persistent, 321
sql_decode
rpki::rpki_engine::ca_detail_obj, 282
rpki::sql::sql_persistent, 317
sql_delete
rpki::sql::sql_persistent, 318
sql_delete_hook
rpki::rpki_engine::roa_obj, 303
rpki::sql::sql_persistent, 318
sql_deleted
rpki::sql::sql_persistent, 321
sql_encode
rpki::sql::sql_persistent, 318
sql_fetch
rpki::sql::sql_persistent, 318
sql_fetch_all
rpki::sql::sql_persistent, 319
sql_fetch_hook
rpki::rpki_engine::roa_obj, 303
rpki::sql::sql_persistent, 319
sql_fetch_where
rpki::sql::sql_persistent, 319
sql_fetch_where1
rpki::sql::sql_persistent, 319
sql_in_db
rpki::sql::sql_persistent, 322
sql_init
rpki::sql::sql_persistent, 319
sql_insert_hook
rpki::rpki_engine::roa_obj, 303
rpki::sql::sql_persistent, 320
sql_is_dirty
rpki::sql::sql_persistent, 320
sql_mark_clean
rpki::sql::sql_persistent, 320
sql_mark_deleted

rpki::sql::sql_persistent, 320
sql_mark_dirty
rpki::sql::sql_persistent, 320
sql_store
rpki::sql::sql_persistent, 321
sql_template
rpki::left_right::bsc_elt, 186
rpki::left_right::child_elt, 190
rpki::left_right::parent_elt, 207
rpki::left_right::repository_elt, 212
rpki::left_right::self_elt, 220
rpki::publication::client_elt, 229
rpki::publication::con g_elt, 233
rpki::rpki_engine::ca_detail_obj, 285
rpki::rpki_engine::ca_obj, 291
rpki::rpki_engine::child_cert_obj, 295
rpki::rpki_engine::revoked_cert_obj, 300
rpki::rpki_engine::roa_obj, 305
sql_update_hook
rpki::sql::sql_persistent, 321
stack
rpki::xml_utils::sax_handler, 411
start
rpki::https::http_client, 158
start_cron
rpki::rpki_engine::rpkid_context, 309
startElement
rpki::left_right::list_resources_elt, 198
rpki::left_right::list_roa_requests_-elt, 200
rpki::publication::con g_elt, 232
rpki::up_down::base_elt, 334
rpki::up_down::certi cate_elt, 335
rpki::up_down::class_elt, 338
rpki::up_down::class_response_-syntax, 341
rpki::up_down::issue_pdu, 346
rpki::up_down::message_pdu, 352
rpki::up_down::revoke_syntax, 357
rpki::xml_utils::base_elt, 400
rpki::xml_utils::msg, 408
rpki::xml_utils::sax_handler, 410
startElementNS
rpki::xml_utils::sax_handler, 411
startup_msg
irdbd, 53
state
rpki::https::http_client, 159
rpki::rpki_engine::ca_detail_obj, 285
status
rpki::up_down::error_response_pdu, 345
suggested_sia_head
rpki::up_down::class_elt, 340
sundial.py(2785), 427
sweep
rpki::sql::session, 315
symmetric_difference
rpki::resource_set::resource_set, 258

ta
rpki::https::http_client, 159
rpki::https::http_listener, 161
rpki::https::http_queue, 167
table
rpki::sql::template, 324
tag
rpki::left_right::report_error_elt, 209
rpki::log, 77
rpki::publication::report_error_elt, 244
test
rpki::sundial, 88
test1
rpki::resource_set, 84
test2
rpki::resource_set, 84
text
rpki::xml_utils::sax_handler, 411
text_attribute
rpki::left_right::list_published_-objects_elt, 197
rpki::left_right::report_error_elt, 209
rpki::publication::report_error_elt, 244
rpki::xml_utils::text_elt, 413

textwrap::TextWrapper, 413
thisUpdate
    rpki::manifest::Manifest, 225
timeout
    rpki::https::http_client, 159
    rpki::https::http_server, 173
timer
    rpki::async::gc_summary, 124
    rpki::https::http_stream, 179
tls
    rpki::https::http_client, 159
    rpki::https::http_server, 173
    rpki::https::http_stream, 179
tls_accept
    rpki::https::http_server, 172
tls_connect
    rpki::https::http_client, 158
to_bytes
    rpki::ipaddrs::v4addr, 180
    rpki::ipaddrs::v6addr, 182
to_DER
    rpki::x509::PEM_converter, 378
to_PEM
    rpki::x509::PEM_converter, 378
to_resource_bag
    rpki::up_down::class_elt, 338
to_resource_range
    rpki::resource_set::roa_pre x, 266
to_resource_set
    rpki::resource_set::roa_pre x_set, 270
to_rfc3779_tuple
    rpki::resource_set::resource_range_as, 252
    rpki::resource_set::resource_range_ip, 254
    rpki::resource_set::resource_set_as, 260
    rpki::resource_set::resource_set_ip, 262
to_roa_tuple
    rpki::resource_set::roa_pre x, 267
    rpki::resource_set::roa_pre x_set, 270
to_sql
    rpki::sundial::datetime, 327
    rpki::x509::DER_object, 376
toASN1tuple
    rpki::sundial::datetime, 327
toGeneralizedTime
    rpki::sundial::datetime, 327
top_opts
    irbe_cli, 48
totimestamp
    rpki::sundial::datetime, 328
toUTCTime
    rpki::sundial::datetime, 328
toXML
    rpki::left_right::list_resources_elt, 198
    rpki::publication::publication_object_elt, 241
    rpki::up_down::certi cate_elt, 336
    rpki::up_down::class_elt, 338
    rpki::up_down::class_response_syntax, 341
    rpki::up_down::error_response_pdu, 344
    rpki::up_down::issue_pdu, 346
    rpki::up_down::list_pdu, 349
    rpki::up_down::message_pdu, 352
    rpki::up_down::revoke_syntax, 357
    rpki::xml_utils::base_elt, 401
    rpki::xml_utils::data_elt, 405
    rpki::xml_utils::msg, 408
    rpki::xml_utils::text_elt, 412
toXMLtime
    rpki::sundial::datetime, 328
trace
    rpki::async::timer, 132
    rpki::log, 75
traceback
    rpki::log, 76
type
    rpki::up_down::message_pdu, 353
    rpki::xml_utils::msg, 408
type2name
    rootd::message_pdu, 121
    rpki::up_down::message_pdu, 353

u
    irdbd, 53

undersized
rpki::resource_set::resource_bag, 249
unimplemented_control
rpki::xml_utils::data_elt, 405
union
rpki::resource_set::resource_bag, 249
rpki::resource_set::resource_set, 259
unwind_stack
rpki::async::iterator, 126
unwrap
rpki::x509::XML_CMS_object, 397
up_down
rpki::relaxng, 81
up_down.py(2935), 428
up_down_handler
rootd, 58
rpki::rpki_engine::rpkid_context, 309
up_down_url_regexp
rpki::rpki_engine::rpkid_context, 312
update
rpki::rpki_engine::ca_detail_obj, 282
rpki::rpki_engine::roa_obj, 303
rpki::sql::template, 324
update_children
rpki::left_right::self_elt, 218
update_roas
rpki::left_right::self_elt, 219
update_timeout
rpki::https::http_stream, 177
uri
rpki::rpki_engine::child_cert_obj, 293
rpki::rpki_engine::roa_obj, 304
uri_tail
rpki::rpki_engine::child_cert_obj, 294
rpki::rpki_engine::roa_obj, 304
uri_to_ lename
rpki::publication::publication_-object_elt, 241
uris
rpki::rpki_engine::publication_-queue, 297
url
irbe_cli::caller, 99
usage
irbe_cli, 46
irbe_cli::cmd_elt_mixin, 102
irbe_cli::cmd_msg_mixin, 104
usage_ ll
irbe_cli, 48
use_hsm
rpki::left_right::self_elt, 221
use_internal_cron
rpki::rpki_engine::rpkid_context, 312
use_syslog
rpki::log, 77
username
rpki::sql::session, 316

v4
rpki::resource_set::resource_bag, 249
v6
rpki::resource_set::resource_bag, 249
valid_until
rpki::left_right::list_resources_elt, 199
rpki::resource_set::resource_bag, 250
verbose
irbe_cli, 48
verify
rpki::x509::CMS_object, 362
version
rpki::https::http_message, 164
rpki::left_right::msg, 202
rpki::left_right::sax_handler, 213
rpki::manifest::Manifest, 225
rpki::publication::msg, 237
rpki::publication::sax_handler, 246
rpki::roa::RouteOriginAttestation, 277
rpki::up_down::message_pdu, 353
rpki::up_down::sax_handler, 359

rpki::xml_utils::msg, 408

want_persistent_client
rpki::https, 71
want_persistent_server
rpki::https, 71
warn
rpki::log, 77
when
rpki::async::timer, 133
wired_in_con g_id
rpki::publication::con g_elt, 233
withdraw
rpki::rpki_engine::publication_-
queue, 296
wrap
rpki::x509::XML_CMS_object, 397
writeable
rpki::https::http_stream, 178

x509.py(2928), 428
xml::sax::handler::ContentHandler, 414
xml_utils.py(2836), 429
xmlns
rpki::left_right::left_right_-
namespace, 195
rpki::publication::publication_-
namespace, 238
rpki::up_down, 90