RPKI Engine

1.0

Generated by Doxygen 1.5.5

Thu Jun 12 18:21:05 2008

Contents

1 RPKI Engine Reference Manual 1

2 Installation 1

3 Operation 3

4 Left-right protocol 16

5 Publication protocol 26

6 Namespace Documentation 30

7 Class Documentation 53

8 File Documentation 386

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 documentation you're reading is generated automatically by Doxygen from comments and documentation in the code.

This work is funded by ARIN, in collaboration with the other RIRs. 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

Besides the automatically-generated code documentation, this manual also includes several sections documenting the overall package:

- The installation instructions

- The operation instructions
- A description of the left-right protocol
- A description of the publication protocol

2 Installation

Preliminary installation 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.

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

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

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

The first step to running the code is to build the OpenSSL and POW binaries. At present the OpenSSL code is just a copy of the stock OpenSSL 0.9.8g release, compiled with special options to enable RFC 3779 support that ISC wrote under previous contract to ARIN. The POW (Python OpenSSL Wrapper) library is an extended copy of the stock POW release.

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

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

This should automatically build everything, in the right order, including staticly linking the POW extension module with the OpenSSL library to provide RFC 3779 support.

Next, see the list of required Python modules in rpkid/README. Note that the Python code requires Python version 2.5. Install any modules that might be missing.

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.

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

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

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

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

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

3 Operation

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

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

Basic operation consists of creating the appropriate MySQL databases, starting rpkid, 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 publication protocol isn't fully specified yet, much less implmenented. At the moment rpkid just writes its outputs to a local directory tree.

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 has to 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.

3.1 rpkid.py

rpkid is the main RPKI engine daemon. Configuration of rpkid is a two step process: a config file to bootstrap rpkid to the point where it can speak using the left-right protocol, followed by dynamic configuration via the left-right protocol. 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 config file is rpkid.conf, start rpkid with "-c filename" to choose a different config file. All options are in the section "[rpkid]". 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 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.
- `cms-ta-irdb`: Name of file containing CMS trust anchor to use when authenticating messages from irdbd.
- `cms-ta-irbe`: Name of file containing CMS trust anchor to use when authenticating control messages from IRBE.
- `cms-key`: Name of file containing RSA key to use when signing CMS messages to IRBE or irdbd.
- `cms-cert`: Name(s) of file(s) containing certificate(s) to include in CMS wrapper when signing messages to IRBE or irdbd. You can specify more than one certificate using OpenSSL-style subscripts: cms-cert.0, cms-cert.1, etc.
- `https-key`: Name of file containing RSA key to use, both in the HTTPS server role (for both up-down and left-right protocols) and in the HTTPS client role (left-right protocol only).

- `https-cert`: Name(s) of file(s) containing certificate(s) to use in same contexts where https-key is used. You can specify more than one certificate using OpenSSL-style subscripts: https-cert.0, https-cert.1, etc.

- `https-ta`: Name of file containing trust anchor to use when verifying irdbd's HTTPS server certificate.

- `irdb-url`: Service URL for irdbd. Must be a https:// URL.

- `https-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.

- `https-server-port`: TCP port on which to listen for HTTPS connections.

3.2 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]". Certifiates, 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/".

3.3 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:

- `cms-ta`: Name of file containing trust anchor to use when verifying CMS up-down queries.

- `cms-key`: Name of file containing RSA key to use when signing CMS up-down replies.
- `cms-cert`: Name(s) of file(s) containing certificate(s) to include in CMS wrapper when signing up-down replies. You can specify more than one certificate using OpenSSL-style subscripts: cms-cert.0, cms-cert.1, etc.
- `https-key`: Name of file containing RSA key to use in the HTTPS server role for the up-down protocol.
- `https-cert`: Name(s) of file(s) containing certificate(s) to use in the HTTPS server role for the up-down protocol. You can specify more than one certificate using OpenSSL-style subscripts: https-cert.0, https-cert.1, etc.
- `https-server-host`: Hostname or IP address on which to listen for HTTPS connections. Default is localhost.
- `https-server-port`: TCP port on which to listen for HTTPS connections.
- `rpki-key`: Name of file containing RSA key to use in signing resource certificates.
- `rpki-issuer`: Name of file containing self-signed root resource certificate corresponding to rpki-key.
- `rpki-subject-filename`: Name of file that rootd should use to save the one and only certificate it issues.
- `rpki-pkcs10-filename`: 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.

3.4 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.
- `cms-ta`: Name of file containing CMS trust anchor to use when authenticating messages from rpkid.
- `cms-key`: Name of file containing RSA key to use when signing CMS messages to rpkid.
- `cms-cert`: Name(s) of file(s) containing certificate(s) to include in CMS wrapper when signing messages to rpkid. You can specify more than one certificate using OpenSSL-style subscripts: cms-cert.0, cms-cert.1, etc.
- `https-key`: Name of file containing RSA key to use in the HTTPS server role when listening for connections from rpkid.
- `https-cert`: Name(s) of file(s) containing certificate(s) to use in the HTTPS server role when listening for connections from rpkid. You can specify more than one certificate using OpenSSL-style subscripts: https-cert.0, https-cert.1, etc.
- `https-url`: Service URL for irdbd. Must be a https:// URL.

3.5 irbe-cli.py

irbe-cli is a simple command line client for the control subset of the left-right protocol. In production use this functionality would be part of the IRBE stub.

Basic configuration of irbe-cli is handled via a config file. The specific action or actions to be performed are specified on the command line, and map closely to the left-right protocol itself.

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

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

Usage:

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

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

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

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

`-action` is one of `create`, `set`, `get`, `list`, or `destroy`; exactly one of these must be specified for each command.

`-type` is `query` or `reply`; since irbe-cli is a client, `query` is the default.

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

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

The remaining options are specific to the particular commands, and follow directly from the left-right protocol specification.

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

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

Config file options:

- `cms-ta`: Name of file containing CMS trust anchor to use when authenticating messages from rpkid.
- `cms-key`: Name of file containing RSA key to use when signing CMS messages to rpkid.
- `cms-cert`: Name(s) of file(s) containing certificate(s) to include in CMS wrapper when signing messages to rpkid. You can specify more than one certificate using OpenSSL-style subscripts: cms-cert.0, cms-cert.1, etc.
- `https-key`: Name of file containing RSA key to use in the HTTPS client role when contacting rpkid.
- `https-cert`: Name(s) of file(s) containing certificate(s) to use in the HTTPS client role when contacting rpkid. You can specify more than one certificate using OpenSSL-style subscripts: https-cert.0, https-cert.1, etc.
- `https-ta`: Name of file containing trust anchor to use when verifying rpkid's HTTPS server certificate.
- `https-url`: Service URL for rpkid. Must be a https:// URL.

3.6 irbe-setup.py config file

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:

- `cms-ta`: Name of file containing CMS trust anchor to use when authenticating messages from rpkid.
- `cms-key`: Name of file containing RSA key to use when signing CMS messages to rpkid.
- `cms-cert`: Name(s) of file(s) containing certificate(s) to include in CMS wrapper when signing messages to rpkid. You can specify more than one certificate using OpenSSL-style subscripts: cms-cert.0, cms-cert.1, etc.
- `https-key`: Name of file containing RSA key to use in the HTTPS client role when contacting rpkid.
- `https-cert`: Name(s) of file(s) containing certificate(s) to use in the HTTPS client role when contacting rpkid. You can specify more than one certificate using OpenSSL-style subscripts: https-cert.0, https-cert.1, etc.
- `https-ta`: Name of file containing trust anchor to use when verifying rpkid's HTTPS server 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.

3.7 cronjob.py

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

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

Config file options:

- `https-key`: Name of file containing RSA key to use in the HTTPS client role when contacting rpkid.

- `https-cert`: Name(s) of file(s) containing certificate(s) to use in the HTTPS client role when contacting rpkid. You can specify more than one certificate using OpenSSL-style subscripts: https-cert.0, https-cert.1, etc.

- `https-ta`: Name of file containing trust anchor to use when verifying rpkid's HTTPS server certificate.

- `https-url`: Service URL for rpkid. Must be a https:// URL.

3.8 testbed.py:

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

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

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

testbed.conf options:

- `testbed_dir`: Working directory into which testbed should write the (many) files it generates. Default is "testbed.dir".

- `irdb_db_pass`: MySQL password for the "irdb" user. Default is "fnord". You may want to override this.

- `rpki_db_pass`: MySQL password for the "rpki" user. Default is "fnord". You may want to override this.

- `rootd_sia`: rsync URI naming a (perhaps fictious) directory to use as the id-ad-caRepository SIA value in the generated root resource certificate. Default is

"rsync://wombat.invalid/". You may want to override this if you intend to run an rsync server and test against the generated results using rcynic. This default will likely change if and when testbed learns how to run rcynic itself as part of the test suite.

The second configuration file is named testbed.yaml by default, run testbed with "-y filename" to change it. The YAML file contains multiple YAML "documents". The first document describes the initial test layout and resource allocations, subsequent documents describe modifications to the initial allocations and other parameters. Resources listed in the initial layout are aggregated automatically, so that a node in the resource hierarchy automatically receives the resources it needs to issue whatever its children are listed as holding. Actions in the subsequent documents are modifications to the current resource set, modifications to validity dates or other non-resource parameters, or special commands like "sleep". The details are still evolving, but here's an example of current usage:

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

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

Operators in subsequent (update) documents:

- `add_as`, `add_v4`, `add_v6`: These add ASN, IPv4, or IPv6 resources, respectively.
- `sub_as`, `sub_v4`, `sub_v6`: These subtract resources.
- `valid_until`: Set an absolute expiration date.
- `valid_for`: Set a relative expiration date.
- `valid_add`, `valid_sub`: Add to or subtract from validity interval.
- `sleep` [interval]: Sleep for specified interval, or until testbed receives a SIGALRM signal.

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

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

3.9 testpoke.py

This is a command-line client for the up-down protocol. Unlike all of the above programs, testpoke does not accept a config file in OpenSSL-compatable format at all. Instead, it is configured 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 configuration language to simplify scripted testing. There are minor variations due to slightly different feature sets, but YAML files intended for one program will usually work with the other.

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

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

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

Default configuration file is testpoke.yaml, override with –yaml option.

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

Sample configuration file:

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

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

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

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

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

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

4 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.

4.1 Terminology

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

4.2 initiated by the IRBE

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

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

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

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

4.2.1 <self/> object

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

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

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

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

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

- `use_hsm` (attribute): Whether to use a Hardware Signing Module. At present this option has no effect, as the implementation does not yet support HSMs.

- `crl_interval` (attribute): Positive integer representing the planned lifetime of an RPKI CRL for this `<self/>`, measured in seconds.

- `regen_margin` (attribute): Positive integer representing how long before expiration of an RPKI certificiate a new one should be generated, measured in seconds. At present this only affects the one-off EE certificates associated with ROAs.

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

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

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

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

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

4.2.2 <bsc/> object

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

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

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

- `signing_cert` (element): BPKI certificate to use when generating a signature.

- `signing_cert_crl` (element): CRL which would list signing_cert if it had been revoked.

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

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

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

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

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

4.2.3 <parent/> object

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

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

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

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

- `recipient_name` (attribute): Recipient name to use in the up-down protocol when talking to this parent. The RPKI engine doesn't really care what this value is, but other implementations of the up-down protocol do care.

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

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

- `bpki_https_cert` (element): BPKI HTTPS CA certificate for this `<parent/>`. This is like the bpki_cms_cert object, only used for validating incoming TLS messages rather than CMS.

- `bpki_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.

4.2.4 <child/> object

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

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

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

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

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

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

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

4.2.5 <repository/> object

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

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

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

- peer_contact_uri (attribute): HTTPS URI used to contact this repository.

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

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

- bpki_https_cert (element): BPKI HTTPS CA certificate for this <repository/>. This is like the bpki_cms_cert object, only used for validating incoming TLS messages rather than CMS.

- bpki_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.

4.2.6 <route_origin/> object

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

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

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

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

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

- ipv4 (attribute): List of IPv4 prefix and maxLength values, see below for format.

- ipv6 (attribute): List of IPv6 prefix and maxLength values, see below for format.

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

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

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

ABNF for these address lists:

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

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

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

4.3 Operations initiated by the RPKI engine

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

4.3.1 <list_resources/> messages

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

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

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

- `subject_name`: An optional text string naming the child. Not currently used.
- `asn`: A list of autonomous sequence numbers, expressed as a comma-separated sequence of decimal integers with no whitespace.
- `ipv4`: A list of IPv4 address prefixes and ranges, expressed as a comma-separated list of prefixes and ranges with no whitespace. See below for format details.
- `ipv6`: A list of IPv6 address prefixes and ranges, expressed as a comma-separated list of prefixes and ranges with no whitespace. See below for format details.

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

4.4 Error handling

Error in this protocol are handled at two levels.

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

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

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

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

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

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

5 Publication protocol

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

The first is a configuration protocol for the IRBE to use to configure the 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.

5.1 Terminology

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

5.2 Publication control subprotocol

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

5.2.1 <config/> object

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

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

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

- `bpki_crl` (element): This is the BPKI CRL used by the publication server when signing the CMS wrapper on responses in the publication subprotocol. As the CRL must be updated at regular intervals, it's not practical to restart the publication server when the BPKI CRL needs to be updated. Fortunately, 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.

5.2.2 <client/> object

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

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

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

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

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

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

5.3 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.

5.3.1 <certificate/> object

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

5.3.2 <crl/> object

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

5.3.3 <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.

5.3.4 <roa/> object

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

5.4 Error handling

Error in this protocol are handled at two levels.

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

Where possible, errors will result in a <report_error/> message which takes the place of the expected protocol response message. <report_error/> messages are CMS-

signed XML messages like the rest of this protocol, and thus can be archived to provide an audit trail.

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

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

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

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

5.5 Additional access control considerations.

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

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

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

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

In this case, one could argue that the publication server is responsible for preventing one of its clients (the child in the above description) from stomping on data published by another of its clients (the parent in the above description). This goes beyond the basic access check and requires the publication server to determine whether the parent has given its consent for the child to publish under the parent. Since the RPKI certificate profile requires the child's publication point to be indicated in an SIA extension in

a certificate issued by the parent to the child, the publication engine can infer this permission from the parent's issuance of a certificate to the child. Since, by definition, the parent also uses this publication server, this is an easy check, as the publication server should already have the parent's certificate available by the time it needs to check the child's certificate.

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

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

6 Namespace Documentation

6.1 Package pubd

Classes

- class pubd_context

Functions

- def main

Variables

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

6.1.1 Function Documentation

6.1.1.1 def pubd.main ()

Definition at line 127 of file pubd.py.

6.1.2 Variable Documentation

6.1.2.1 pubd.cfg_file = "pubd.conf"

Definition at line 112 of file pubd.py.

6.1.2.2 pubd.profile = False

Definition at line 113 of file pubd.py.

6.2 Package rpki

Packages

- package config
- package exceptions
- package https
- package ipaddrs
- package left_right
- package log
- package manifest
- package oids
- package publication
- package relaxng
- package resource_set
- package roa
- package rpki_engine
- package sql
- package sundial
- package up_down
- package x509
- package xml_utils

6.3 Package rpki.config

Classes

- class parser

6.3.1 Detailed Description

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

$Id: config.py 1873 2008-06-12 02:49:41Z 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.
```

6.4 Package rpki.exceptions

Classes

- class BadClassNameSyntax
- class BadContactURL
- class BadIRDBReply
- class BadIssueResponse
- class BadPKCS10
- class BadQuery
- class BadSender
- class BadStatusCode
- class BadURISyntax
- class BSCNotFound
- class ChildNotFound
- class ClassNameMismatch
- class CMSCRLNotSet
- class CMSVerificationFailed
- class DBConsistancyError
- class DERObjectConversionError
- class EmptyPEM
- class HTTPRequestFailed
- class MissingCMSCRL
- class MissingCMSEEcert
- class MultipleTLSEECert
- class MustBePrefix

- class NotACertificateChain
- class NotFound
- class NotImplementedYet
- class NotInDatabase
- class ReceivedTLSCACert
- class RPKI_Exception
- class ServerShuttingDown
- class SKIMismatch
- class SubprocessError
- class TLSValidationError
- class UnexpectedCMSCerts
- class UnexpectedCMSCRLs
- class UnparsableCMSDER
- class UpstreamError
- class WrongEContentType

6.4.1 Detailed Description

```
Exception definitions for RPKI modules.

$Id: exceptions.py 1873 2008-06-12 02:49:41Z 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.
```

6.5 Package rpki.https

Classes

- class Checker
- class httpsClient
- class httpsServer
- class requestHandler

Functions

- def build_https_ta_cache
- def client
- def server
- def tlslite_certChain

Variables

- debug_tls_certs = False
- disable_tls_certificate_validation_exceptions = False
- string rpki_content_type = "application/x-rpki"

6.5.1 Detailed Description

```
HTTPS utilities, both client and server.

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

$Id: https.py 1873 2008-06-12 02:49:41Z 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.
```

6.5.2 Function Documentation

6.5.2.1 def rpki.https.build_https_ta_cache (*certs*)

```
Build a dynamic TLS trust anchor cache.
```

Definition at line 45 of file https.py.

6.5.2.2 def rpki.https.client (*msg*, *client_key*, *client_cert*, *server_ta*, *url*, *timeout* = 300)

```
Open client HTTPS connection, send a message, wait for response.

This function wraps most of what one needs to do to send a message
over HTTPS and get a response.  The certificate checking isn't quite
up to snuff; it's better than with the other packages I've found,
but doesn't appear to handle subjectAltName extensions (sigh).
```

Definition at line 152 of file https.py.

6.5.2.3 def rpki.https.server (*handlers*, *server_key*, *server_cert*, *port* = 4433, *host* = "", *client_ta* = None, *dynamic_https_trust_anchor* = None, *catch_signals* = (signal.SIGINT, signal.SIGTERM)

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

Definition at line 266 of file https.py.

6.5.2.4 def rpki.https.tlslite_certChain (*x509*)

```
Utility function to construct tlslite certChains.
```

Definition at line 38 of file https.py.

6.5.3 Variable Documentation

6.5.3.1 rpki::https.debug_tls_certs = False

Definition at line 34 of file https.py.

6.5.3.2 rpki::https.disable_tls_certificate_validation_exceptions = False

Definition at line 31 of file https.py.

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

Definition at line 36 of file https.py.

6.6 Package rpki.ipaddrs

Classes

- class v4addr
- class v6addr

6.6.1 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 1873 2008-06-12 02:49:41Z 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.
```


6.7 Package rpki.left_right

Classes

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

Variables

- enforce_strict_up_down_xml_sender = False

6.7.1 Detailed Description

```
RPKI "left-right" protocol.

$Id: left_right.py 1873 2008-06-12 02:49:41Z 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.
```

6.7.2 Variable Documentation

6.7.2.1 rpki::left_right.enforce_strict_up_down_xml_sender = False

Definition at line 26 of file left_right.py.

6.8 Package rpki.log

Classes

- class logger

Functions

- def init
- def set_trace
- def trace

Variables

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

Whether call tracing is enabled.

- tuple error = logger(syslog.LOG_ERR)
- tuple info = logger(syslog.LOG_INFO)
- tuple note = logger(syslog.LOG_NOTICE)
- tuple warn = logger(syslog.LOG_WARNING)

6.8.1 Detailed Description

```
Logging facilities for RPKI libraries.

$Id: log.py 1873 2008-06-12 02:49:41Z 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.
```

6.8.2 Function Documentation

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

```
Initialize logging system.
```

Definition at line 27 of file log.py.

6.8.2.2 def rpki.log.set_trace (*trace*)

```
Enable or disable call tracing.
```

Definition at line 32 of file log.py.

6.8.2.3 def rpki.log.trace ()

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

Definition at line 53 of file log.py.

6.8.3 Variable Documentation

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

Definition at line 51 of file log.py.

6.8.3.2 rpki::log::enable_trace = False

Whether call tracing is enabled.

Definition at line 25 of file log.py.

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

Definition at line 47 of file log.py.

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

Definition at line 50 of file log.py.

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

Definition at line 49 of file log.py.

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

Definition at line 48 of file log.py.

6.9 Package rpki.manifest

Classes

- class FileAndHash
- class FilesAndHashes
- class Manifest

6.9.1 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 1873 2008-06-12 02:49:41Z 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.

6.10 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.

6.10.1 Detailed Description

OID database.

$Id: oids.py 1873 2008-06-12 02:49:41Z 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.

6.10.2 Variable Documentation

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

Mapping table of string names to OIDs.

Definition at line 57 of file oids.py.

6.10.2.2 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, 10)         : "id-ad-rpkiManifest",
  (1, 3, 6, 1, 5, 5, 7, 48, 11)         : "id-ad-signedObject",
  (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",
  (2, 16, 840, 1, 101, 3, 4, 2, 1)      : "id-sha256",
  (2, 5, 29, 14)                        : "subjectKeyIdentifier",
  (2, 5, 29, 15)                        : "keyUsage",
  (2, 5, 29, 19)                        : "basicConstraints",
  (2, 5, 29, 20)                        : "cRLNumber",
  (2, 5, 29, 31)                        : "cRLDistributionPoints",
  (2, 5, 29, 32)                        : "certificatePolicies",
  (2, 5, 29, 35)                        : "authorityKeyIdentifier",
  (2, 5, 4, 3)                          : "commonName",
}
```

Mapping table of OIDs to conventional string names.

Definition at line 23 of file oids.py.

6.11 Package rpki.publication

Classes

- class certificate_elt
- class client_elt
- class cms_msg
- class config_elt
- class control_elt
- class crl_elt

- class manifest_elt
- class msg
- class publication_namespace
- class publication_object_elt
- class report_error_elt
- class roa_elt
- class sax_handler

Variables

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

  Map of data types to publication element wrapper types.

6.11.1 Detailed Description

```
RPKI "publication" protocol.

$Id: publication.py 1873 2008-06-12 02:49:41Z 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.
```

6.11.2 Variable Documentation

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

Map of data types to publication element wrapper types.

Definition at line 232 of file publication.py.

6.12 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.

6.12.1 Variable Documentation

6.12.1.1 rpki::relaxng::left_right

Parsed RelaxNG left_right schema.

Definition at line 7 of file relaxng.py.

6.12.1.2 rpki::relaxng::publication

Parsed RelaxNG publication schema.

Definition at line 1214 of file relaxng.py.

6.12.1.3 rpki::relaxng::up_down

Parsed RelaxNG up_down schema.

Definition at line 960 of file relaxng.py.

6.13 Package rpki.resource_set

Classes

- class resource_bag
- class resource_range
- class resource_range_as
- class resource_range_ip
- class resource_range_ipv4
- class resource_range_ipv6
- class resource_set

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

Functions

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

Variables

- string inherit_token = "<inherit>"

  Token used to indicate inheritance in read and print syntax.

6.13.1 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 1873 2008-06-12 02:49:41Z 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.
```

6.13.2 Function Documentation

6.13.2.1 def rpki.resource_set._bs2long (*bs*) [private]

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

Definition at line 422 of file resource_set.py.

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

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

Definition at line 428 of file resource_set.py.

6.13.2.3 def rpki.resource_set._rsplit (*rset*, *that*) [private]

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

Definition at line 148 of file resource_set.py.

6.13.2.4 def rpki.resource_set.test1 (*t*, *s1*, *s2*)

Definition at line 731 of file resource_set.py.

6.13.2.5 def rpki.resource_set.test2 (*t*, *s1*, *s2*)

Definition at line 764 of file resource_set.py.

6.13.3 Variable Documentation

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

Token used to indicate inheritance in read and print syntax.

Definition at line 33 of file resource_set.py.

6.14 Package rpki.roa

Classes

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

6.14.1 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 1873 2008-06-12 02:49:41Z 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-02 2.1.3.2 specifies:

   RouteOriginAttestation ::= SEQUENCE {
      version [0] INTEGER DEFAULT 0,
      asID  ASID,
      exactMatch BOOLEAN,
      ipAddrBlocks ROAIPAddrBlocks }

   ASID ::= INTEGER

   ROAIPAddrBlocks ::= SEQUENCE of ROAIPAddressFamily

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

   IPAddress ::= BIT STRING
```

```
... but we now implement the new format that will supposedly appear
in the upcoming draft-ietf-sidr-roa-format-03:

   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 ::= {
      address IPAddress,
      maxLength INTEGER OPTIONAL }

   IPAddress ::= BIT STRING
```

6.15 Package rpki.rpki_engine

Classes

- class ca_detail_obj
- class ca_obj
- class child_cert_obj
- class revoked_cert_obj
- class rpkid_context

6.15.1 Detailed Description

```
Global context for rpkid.

$Id: rpki_engine.py 1873 2008-06-12 02:49:41Z 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.
```

6.16 Package rpki.sql

Classes

- class session
- class sql_persistant
- class template

6.16.1 Detailed Description

```
SQL interface code.

$Id: sql.py 1873 2008-06-12 02:49:41Z 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.
```

6.17 Package rpki.sundial

Classes

- class datetime
- class timedelta

Functions

- def now
- def test

6.17.1 Detailed Description

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

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

```
$Id: sundial.py 1873 2008-06-12 02:49:41Z 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.
```

6.17.2 Function Documentation

6.17.2.1 def rpki.sundial.now ()

```
Get current timestamp.
```

Definition at line 26 of file sundial.py.

6.17.2.2 def rpki.sundial.test (*t*)

Definition at line 174 of file sundial.py.

6.18 Package rpki.up_down

Classes

- class base_elt
- class certificate_elt
- class class_elt
- class class_response_syntax
- class cms_msg
- class error_response_pdu
- class issue_pdu
- class issue_response_pdu
- class list_pdu
- class list_response_pdu
- class message_pdu
- class multi_uri
- class revoke_pdu
- class revoke_response_pdu

- class revoke_syntax
- class sax_handler

Variables

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

6.18.1 Detailed Description

```
RPKI "up-down" protocol.

$Id: up_down.py 1873 2008-06-12 02:49:41Z 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.
```

6.18.2 Variable Documentation

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

Definition at line 26 of file up_down.py.

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

Definition at line 24 of file up_down.py.

6.19 Package rpki.x509

Classes

- class CMS_object
- class CRL
- class DER_CMS_object

- class DER_object
- class PEM_converter
- class PKCS10
- class ROA
- class RSA
- class RSApublic
- class SignedManifest
- class X509
- class XML_CMS_object

Functions

- def calculate_SKI
- def POWify_OID

6.19.1 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 1873 2008-06-12 02:49:41Z 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.
```

6.19.2 Function Documentation

6.19.2.1 def rpki.x509.calculate_SKI (*public_key_der*)

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

Definition at line 33 of file x509.py.

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

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

Definition at line 574 of file x509.py.

6.20 Package rpki.xml_utils

Classes

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

6.20.1 Detailed Description

```
XML utilities.

$Id: xml_utils.py 1873 2008-06-12 02:49:41Z 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.
```

6.21 Package rpkid

Functions

- def main

Variables

- string cfg_file = "rpkid.conf"
- profile = None

6.21.1 Function Documentation

6.21.1.1 def rpkid.main ()

Definition at line 52 of file rpkid.py.

6.21.2 Variable Documentation

6.21.2.1 rpkid.cfg_file = "rpkid.conf"

Definition at line 37 of file rpkid.py.

6.21.2.2 rpkid.profile = None

Definition at line 38 of file rpkid.py.

7 Class Documentation

7.1 BaseHTTPRequestHandler Class Reference

Inheritance diagram for BaseHTTPRequestHandler:

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

- https.py (1873)

7.2 HTTPServer Class Reference

Inheritance diagram for HTTPServer:

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

- https.py (1873)

7.3 RawConfigParser Class Reference

Inheritance diagram for RawConfigParser:

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

- config.py (1873)

7.4 Exception Class Reference

Inheritance diagram for Exception:

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

- exceptions.py (1873)

7.5 list Class Reference

Inheritance diagram for list:

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

- resource_set.py (1873)

7.6 long Class Reference

Inheritance diagram for long:

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

- ipaddrs.py (1873)

7.7 object Class Reference

Inheritance diagram for object:

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

- x509.py (1873)

7.8 pubd.pubd_context Class Reference

Inheritance diagram for pubd.pubd_context:

Public Member Functions

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

Public Attributes

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

Static Public Attributes

- https_ta_cache = None
  HTTPS trust anchor cache, to avoid regenerating it for every TLS connection.

7.8.1 Detailed Description

```
A container for various pubd parameters.
```

Definition at line 32 of file pubd.py.

7.8.2 Member Function Documentation

7.8.2.1 def pubd.pubd_context.__init__ (*self*, *cfg*)

Definition at line 35 of file pubd.py.

7.8.2.2 def pubd.pubd_context.build_https_ta_cache (*self*)

```
Build dynamic TLS trust anchors.
```

Definition at line 97 of file pubd.py.

7.8.2.3 def pubd.pubd_context.clear_https_ta_cache (*self*)

```
Clear dynamic TLS trust anchors.
```

Definition at line 90 of file pubd.py.

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

```
Process one PDU from a client.
```

Definition at line 67 of file pubd.py.

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

```
Process one PDU from the IRBE.
```

Definition at line 57 of file pubd.py.

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

```
Common PDU handler code.
```

Definition at line 49 of file pubd.py.

7.8.3 Member Data Documentation

7.8.3.1 pubd.pubd_context.bpki_ta

Definition at line 39 of file pubd.py.

7.8.3.2 pubd.pubd_context.https_server_host

Definition at line 44 of file pubd.py.

7.8.3.3 pubd.pubd_context.https_server_port

Definition at line 45 of file pubd.py.

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

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

Definition at line 88 of file pubd.py.

7.8.3.5 pubd.pubd_context.irbe_cert

Definition at line 40 of file pubd.py.

7.8.3.6 pubd.pubd_context.pubd_cert

Definition at line 41 of file pubd.py.

7.8.3.7 pubd.pubd_context.pubd_key

Definition at line 42 of file pubd.py.

7.8.3.8 pubd.pubd_context.publication_base

Definition at line 47 of file pubd.py.

7.8.3.9 pubd.pubd_context.sql

Definition at line 37 of file pubd.py.

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

- pubd.py (1853)

7.9 datetime Class Reference

Inheritance diagram for datetime:

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

- sundial.py (1873)

7.10 timedelta Class Reference

Inheritance diagram for timedelta:

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

- sundial.py (1873)

7.11 rpki.config.parser Class Reference

Inheritance diagram for rpki.config.parser:

Public Member Functions

- def __init__
- def get
- def multiget

Public Attributes

- default_section

7.11.1 Detailed Description

Definition at line 23 of file config.py.

7.11.2 Member Function Documentation

7.11.2.1 def rpki.config.parser.__init__ (*self*, *file* = `None`, *section* = `None`)

```
Initialize this parser.
```

Definition at line 25 of file config.py.

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

```
Get an option, perhaps with a default value.
```

Definition at line 49 of file config.py.

7.11.2.3 def rpki.config.parser.multiget (*self*, *option*, *section* = `None`)

```
Parse OpenSSL-style foo.0, foo.1, ... subscripted options.

Returns a list of values matching the specified option name.
```

Definition at line 32 of file config.py.

7.11.3 Member Data Documentation

7.11.3.1 rpki.config.parser.default_section

Definition at line 30 of file config.py.

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

- config.py (1873)

7.12 rpki.exceptions.BadClassNameSyntax Class Reference

Inheritance diagram for rpki.exceptions.BadClassNameSyntax:

7.12.1 Detailed Description

```
Illegal syntax for a class_name.
```

Definition at line 53 of file exceptions.py.

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

- exceptions.py (1873)

7.13 rpki.exceptions.BadContactURL Class Reference

Inheritance diagram for rpki.exceptions.BadContactURL:

7.13.1 Detailed Description

```
Error trying to parse up-down protocol contact URL.
```

Definition at line 50 of file exceptions.py.

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

- exceptions.py (1873)

7.14 rpki.exceptions.BadIRDBReply Class Reference

Inheritance diagram for rpki.exceptions.BadIRDBReply:

7.14.1 Detailed Description

```
Unexpected reply to IRDB query.
```

Definition at line 86 of file exceptions.py.

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

- exceptions.py (1873)

7.15 rpki.exceptions.BadIssueResponse Class Reference

Inheritance diagram for rpki.exceptions.BadIssueResponse:

7.15.1 Detailed Description

`issue_response PDU with wrong number of classes or certificates.`

Definition at line 56 of file exceptions.py.

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

- exceptions.py (1873)

7.16 rpki.exceptions.BadPKCS10 Class Reference

Inheritance diagram for rpki.exceptions.BadPKCS10:

7.16.1 Detailed Description

```
Bad PKCS #10 object.
```

Definition at line 62 of file exceptions.py.

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

- exceptions.py (1873)

7.17 rpki.exceptions.BadQuery Class Reference

Inheritance diagram for rpki.exceptions.BadQuery:

7.17.1 Detailed Description

```
Unexpected protocol query.
```

Definition at line 32 of file exceptions.py.

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

- exceptions.py (1873)

7.18 rpki.exceptions.BadSender Class Reference

Inheritance diagram for rpki.exceptions.BadSender:

7.18.1 Detailed Description

```
Unexpected XML sender value.
```

Definition at line 74 of file exceptions.py.

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

- exceptions.py (1873)

7.19 rpki.exceptions.BadStatusCode Class Reference

Inheritance diagram for rpki.exceptions.BadStatusCode:

7.19.1 Detailed Description

```
Unrecognized protocol status code.
```

Definition at line 29 of file exceptions.py.

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

- exceptions.py (1873)

7.20 rpki.exceptions.BadURISyntax Class Reference

Inheritance diagram for rpki.exceptions.BadURISyntax:

7.20.1 Detailed Description

```
Illegal syntax for a URI.
```

Definition at line 26 of file exceptions.py.

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

- exceptions.py (1873)

7.21 rpki.exceptions.BSCNotFound Class Reference

Inheritance diagram for rpki.exceptions.BSCNotFound:

7.21.1 Detailed Description

```
Could not find specified BSC in database.
```

Definition at line 71 of file exceptions.py.

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

- exceptions.py (1873)

7.22 rpki.exceptions.ChildNotFound Class Reference

Inheritance diagram for rpki.exceptions.ChildNotFound:

7.22.1 Detailed Description

```
Could not find specified child in database.
```

Definition at line 68 of file exceptions.py.

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

- exceptions.py (1873)

7.23 rpki.exceptions.ClassNameMismatch Class Reference

Inheritance diagram for rpki.exceptions.ClassNameMismatch:

7.23.1 Detailed Description

```
class_name does not match child context.
```

Definition at line 77 of file exceptions.py.

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

- exceptions.py (1873)

7.24 rpki.exceptions.CMSCRLNotSet Class Reference

Inheritance diagram for rpki.exceptions.CMSCRLNotSet:

7.24.1 Detailed Description

```
CMS CRL has not been configured.
```

Definition at line 125 of file exceptions.py.

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

- exceptions.py (1873)

7.25 rpki.exceptions.CMSVerificationFailed Class Reference

Inheritance diagram for rpki.exceptions.CMSVerificationFailed:

7.25.1 Detailed Description

```
Verification of a CMS message failed.
```

Definition at line 38 of file exceptions.py.

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

- exceptions.py (1873)

7.26 rpki.exceptions.DBConsistancyError Class Reference

Inheritance diagram for rpki.exceptions.DBConsistancyError:

7.26.1 Detailed Description

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

Definition at line 35 of file exceptions.py.

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

- exceptions.py (1873)

7.27 rpki.exceptions.DERObjectConversionError Class Reference

Inheritance diagram for rpki.exceptions.DERObjectConversionError:

7.27.1 Detailed Description

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

Definition at line 44 of file exceptions.py.

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

- exceptions.py (1873)

7.28 rpki.exceptions.EmptyPEM Class Reference

Inheritance diagram for rpki.exceptions.EmptyPEM:

7.28.1 Detailed Description

```
Couldn't find PEM block to convert.
```

Definition at line 107 of file exceptions.py.

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

- exceptions.py (1873)

7.29 rpki.exceptions.HTTPRequestFailed Class Reference

Inheritance diagram for rpki.exceptions.HTTPRequestFailed:

7.29.1 Detailed Description

```
HTTP request failed.
```

Definition at line 41 of file exceptions.py.

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

- exceptions.py (1873)

7.30 rpki.exceptions.MissingCMSCRL Class Reference

Inheritance diagram for rpki.exceptions.MissingCMSCRL:

7.30.1 Detailed Description

```
Didn't receive CMS CRL when expecting one.
```

Definition at line 119 of file exceptions.py.

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

- exceptions.py (1873)

7.31 rpki.exceptions.MissingCMSEEcert Class Reference

Inheritance diagram for rpki.exceptions.MissingCMSEEcert:

7.31.1 Detailed Description

```
Didn't receive CMS EE cert when expecting one.
```

Definition at line 116 of file exceptions.py.

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

- exceptions.py (1873)

7.32 rpki.exceptions.MultipleTLSEECert Class Reference

Inheritance diagram for rpki.exceptions.MultipleTLSEECert:

7.32.1 Detailed Description

```
Received more than one TLS EE certificate.
```

Definition at line 98 of file exceptions.py.

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

- exceptions.py (1873)

7.33 rpki.exceptions.MustBePrefix Class Reference

Inheritance diagram for rpki.exceptions.MustBePrefix:

7.33.1 Detailed Description

```
Resource range cannot be expressed as a prefix.
```

Definition at line 92 of file exceptions.py.

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

- exceptions.py (1873)

7.34 rpki.exceptions.NotACertificateChain Class Reference

Inheritance diagram for rpki.exceptions.NotACertificateChain:

7.34.1 Detailed Description

```
Certificates don't form a proper chain.
```

Definition at line 47 of file exceptions.py.

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

- exceptions.py (1873)

7.35 rpki.exceptions.NotFound Class Reference

Inheritance diagram for rpki.exceptions.NotFound:

7.35.1 Detailed Description

```
Object not found in database.
```

Definition at line 89 of file exceptions.py.

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

- exceptions.py (1873)

7.36 rpki.exceptions.NotImplementedYet Class Reference

Inheritance diagram for rpki.exceptions.NotImplementedYet:

7.36.1 Detailed Description

```
Internal error -- not implemented yet.
```

Definition at line 59 of file exceptions.py.

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

- exceptions.py (1873)

7.37 rpki.exceptions.NotInDatabase Class Reference

Inheritance diagram for rpki.exceptions.NotInDatabase:

7.37.1 Detailed Description

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

Definition at line 23 of file exceptions.py.

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

- exceptions.py (1873)

7.38 rpki.exceptions.ReceivedTLSCACert Class Reference

Inheritance diagram for rpki.exceptions.ReceivedTLSCACert:

7.38.1 Detailed Description

```
Received CA certificate via TLS.
```

Definition at line 101 of file exceptions.py.

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

- exceptions.py (1873)

7.39 rpki.exceptions.RPKI_Exception Class Reference

Inheritance diagram for rpki.exceptions.RPKI_Exception:

7.39.1 Detailed Description

```
Base class for RPKI exceptions.
```

Definition at line 20 of file exceptions.py.

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

- exceptions.py (1873)

7.40 rpki.exceptions.ServerShuttingDown Class Reference

Inheritance diagram for rpki.exceptions.ServerShuttingDown:

7.40.1 Detailed Description

```
Server is shutting down.
```

Definition at line 128 of file exceptions.py.

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

- exceptions.py (1873)

7.41 rpki.exceptions.SKIMismatch Class Reference

Inheritance diagram for rpki.exceptions.SKIMismatch:

7.41.1 Detailed Description

```
SKI value in response does not match request.
```

Definition at line 80 of file exceptions.py.

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

- exceptions.py (1873)

7.42 rpki.exceptions.SubprocessError Class Reference

Inheritance diagram for rpki.exceptions.SubprocessError:

7.42.1 Detailed Description

```
Subprocess returned unexpected error.
```

Definition at line 83 of file exceptions.py.

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

- exceptions.py (1873)

7.43 rpki.exceptions.TLSValidationError Class Reference

Inheritance diagram for rpki.exceptions.TLSValidationError:

7.43.1 Detailed Description

```
TLS certificate validation error.
```

Definition at line 95 of file exceptions.py.

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

- exceptions.py (1873)

7.44 rpki.exceptions.UnexpectedCMSCerts Class Reference

Inheritance diagram for rpki.exceptions.UnexpectedCMSCerts:

7.44.1 Detailed Description

```
Received CMS certs when not expecting any.
```

Definition at line 110 of file exceptions.py.

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

- exceptions.py (1873)

7.45 rpki.exceptions.UnexpectedCMSCRLs Class Reference

Inheritance diagram for rpki.exceptions.UnexpectedCMSCRLs:

7.45.1 Detailed Description

```
Received CMS CRLs when not expecting any.
```

Definition at line 113 of file exceptions.py.

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

- exceptions.py (1873)

7.46 rpki.exceptions.UnparsableCMSDER Class Reference

Inheritance diagram for rpki.exceptions.UnparsableCMSDER:

7.46.1 Detailed Description

```
Alleged CMS DER wasn't parsable.
```

Definition at line 122 of file exceptions.py.

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

- exceptions.py (1873)

7.47 rpki.exceptions.UpstreamError Class Reference

Inheritance diagram for rpki.exceptions.UpstreamError:

7.47.1 Detailed Description

```
Received an error from upstream.
```

Definition at line 65 of file exceptions.py.

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

- exceptions.py (1873)

7.48 rpki.exceptions.WrongEContentType Class Reference

Inheritance diagram for rpki.exceptions.WrongEContentType:

7.48.1 Detailed Description

```
Received wrong CMS eContentType.
```

Definition at line 104 of file exceptions.py.

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

- exceptions.py (1873)

7.49 rpki.https.Checker Class Reference

Inheritance diagram for rpki.https.Checker:

Public Member Functions

- def __call__
- def __init__
- def x509store_thunk

Public Attributes

- dynamic_https_trust_anchor
- x509store

Static Public Attributes

- pem_dump_tls_certs = False

  Vile debugging hack.

- refuse_tls_ca_certs = False

  Raise an exception upon receiving CA certificates via TLS rather than just quietly ignoring them.

7.49.1 Detailed Description

```
Derived class to handle X.509 client certificate checking.
```

Definition at line 55 of file https.py.

7.49.2 Member Function Documentation

7.49.2.1 def rpki.https.Checker.__call__ (*self*, *tlsConnection*)

```
POW/OpenSSL-based certificate checker.

Given our BPKI model, we're only interested in the TLS EE
certificates.
```

Definition at line 95 of file https.py.

7.49.2.2 def rpki.https.Checker.__init__ (*self*, *trust_anchor* = `None`, *dynamic_https_trust_anchor* = `None`)

```
Initialize our modified certificate checker.
```

Definition at line 69 of file https.py.

7.49.2.3 def rpki.https.Checker.x509store_thunk (*self*)

Definition at line 89 of file https.py.

7.49.3 Member Data Documentation

7.49.3.1 rpki.https.Checker.dynamic_https_trust_anchor

Definition at line 72 of file https.py.

7.49.3.2 rpki::https.Checker::pem_dump_tls_certs = False `[static]`

Vile debugging hack.

Definition at line 67 of file https.py.

7.49.3.3 rpki::https.Checker::refuse_tls_ca_certs = False `[static]`

Raise an exception upon receiving CA certificates via TLS rather than just quietly ignoring them.

Definition at line 62 of file https.py.

7.49.3.4 rpki.https.Checker.x509store

Definition at line 77 of file https.py.

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

- https.py (1873)

7.50 rpki.https.httpsClient Class Reference

Inheritance diagram for rpki.https.httpsClient:

Public Member Functions

- def __init__

Public Attributes

- checker

7.50.1 Detailed Description

```
Derived class to let us replace the default Checker.
```

Definition at line 138 of file https.py.

7.50.2 Member Function Documentation

7.50.2.1 def rpki.https.httpsClient.__init__ (*self*, *host*, *port* = None, *client_cert* = None, *client_key* = None, *server_ta* = None, *settings* = None)

```
Create a new httpsClient.
```

Definition at line 141 of file https.py.

7.50.3 Member Data Documentation

7.50.3.1 rpki.https.httpsClient.checker

Definition at line 148 of file https.py.

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

- https.py (1873)

7.51 rpki.https.httpsServer Class Reference

Inheritance diagram for rpki.https.httpsServer:

Public Member Functions

- def handshake

Static Public Attributes

- rpki_checker = None
- rpki_server_cert = None
- rpki_server_key = None
- rpki_sessionCache = None

7.51.1 Detailed Description

```
Derived type to handle TLS aspects of HTTPS.
```

Definition at line 235 of file https.py.

7.51.2 Member Function Documentation

7.51.2.1 def rpki.https.httpsServer.handshake (*self*, *tlsConnection*)

```
TLS handshake handler.
```

Definition at line 243 of file https.py.

7.51.3 Member Data Documentation

7.51.3.1 rpki.https.httpsServer.rpki_checker = None [static]

Definition at line 241 of file https.py.

7.51.3.2 rpki.https.httpsServer.rpki_server_cert = None [static]

Definition at line 240 of file https.py.

7.51.3.3 rpki.https.httpsServer.rpki_server_key = None [static]

Definition at line 239 of file https.py.

7.51.3.4 rpki.https.httpsServer.rpki_sessionCache = None [static]

Definition at line 238 of file https.py.

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

- https.py (1873)

7.52 rpki.https.requestHandler Class Reference

Inheritance diagram for rpki.https.requestHandler:

Public Member Functions

- def do_POST
- def log_message
- def rpki_find_handler

Static Public Attributes

- rpki_handlers = None

7.52.1 Detailed Description

```
Derived type to supply POST handler and override logging.
```

Definition at line 196 of file https.py.

7.52.2 Member Function Documentation

7.52.2.1 def rpki.https.requestHandler.do_POST (*self*)

```
POST handler.
```

Definition at line 208 of file https.py.

7.52.2.2 def rpki.https.requestHandler.log_message (*self*, *format*, *args*)

```
Redirect HTTP server logging into our own logging system.
```

Definition at line 228 of file https.py.

7.52.2.3 def rpki.https.requestHandler.rpki_find_handler (*self*)

```
Helper method to search self.rpki_handlers.
```

Definition at line 201 of file https.py.

7.52.3 Member Data Documentation

7.52.3.1 rpki.https.requestHandler.rpki_handlers = None [static]

Definition at line 199 of file https.py.

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

- https.py (1873)

7.53 rpki.ipaddrs.v4addr Class Reference

Inheritance diagram for rpki.ipaddrs.v4addr:

Public Member Functions

- def __new__
- def __str__

Static Public Attributes

- int bits = 32

7.53.1 Detailed Description

```
IPv4 address.

Derived from long, but supports IPv4 print syntax.
```

Definition at line 32 of file ipaddrs.py.

7.53.2 Member Function Documentation

7.53.2.1 def rpki.ipaddrs.v4addr.__new__ (*cls*, *x*)

```
Construct a v4addr object.
```

Definition at line 40 of file ipaddrs.py.

7.53.2.2 def rpki.ipaddrs.v4addr.__str__ (*self*)

```
Convert a v4addr object to string format.
```

Definition at line 48 of file ipaddrs.py.

7.53.3 Member Data Documentation

7.53.3.1 int rpki.ipaddrs.v4addr.bits = 32 [static]

Definition at line 38 of file ipaddrs.py.

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

- ipaddrs.py (1873)

7.54 rpki.ipaddrs.v6addr Class Reference

Inheritance diagram for rpki.ipaddrs.v6addr:

Public Member Functions

- def __new__
- def __str__

Static Public Attributes

- int bits = 128

7.54.1 Detailed Description

```
IPv6 address.

Derived from long, but supports IPv6 print syntax.
```

Definition at line 52 of file ipaddrs.py.

7.54.2 Member Function Documentation

7.54.2.1 def rpki.ipaddrs.v6addr.__new__ (*cls*, *x*)

```
Construct a v6addr object.
```

Definition at line 60 of file ipaddrs.py.

7.54.2.2 def rpki.ipaddrs.v6addr.__str__ (*self*)

```
Convert a v6addr object to string format.
```

Definition at line 67 of file ipaddrs.py.

7.54.3 Member Data Documentation

7.54.3.1 int rpki.ipaddrs.v6addr.bits = 128 [static]

Definition at line 58 of file ipaddrs.py.

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

- ipaddrs.py (1873)

7.55 rpki.left_right.bsc_elt Class Reference

Inheritance diagram for rpki.left_right.bsc_elt:

Public Member Functions

- def children
- def parents
- def repositories
- def serve_pre_save_hook

Static Public Attributes

- tuple attributes = ("action", "tag", "self_id", "bsc_id", "key_type", "hash_alg", "key_length")

  XML attributes for this element.

- tuple booleans = ("generate_keypair",)

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

- string element_name = "bsc"
- tuple elements = ("signing_cert", "signing_cert_crl", "pkcs10_request")

  XML elements contained by this element.

- pkcs10_request = None
- private_key_id = None
- signing_cert = None
- signing_cert_crl = None
- tuple sql_template

7.55.1 Detailed Description

```
<bsc/> (Business Signing Context) element.
```

Definition at line 235 of file left_right.py.

7.55.2 Member Function Documentation

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

```
Fetch all child objects that link to this BSC object.
```

Definition at line 262 of file left_right.py.

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

```
Fetch all parent objects that link to this BSC object.
```

Definition at line 258 of file left_right.py.

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

```
Fetch all repository objects that link to this BSC object.
```

Definition at line 254 of file left_right.py.

7.55.2.4 def rpki.left_right.bsc_elt.serve_pre_save_hook (*self*, *q_pdu*, *r_pdu*)

```
Extra server actions for bsc_elt -- handle key generation.
For now this only allows RSA with SHA-256.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 266 of file left_right.py.

7.55.3 Member Data Documentation

7.55.3.1 tuple rpki.left_right.bsc_elt.attributes = ("action", "tag", "self_id", "bsc_id", "key_type", "hash_alg", "key_length") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 239 of file left_right.py.

7.55.3.2 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 241 of file left_right.py.

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

Definition at line 238 of file left_right.py.

7.55.3.4 tuple rpki.left_right.bsc_elt.elements = ("signing_cert", "signing_cert_crl", "pkcs10_request") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 240 of file left_right.py.

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

Definition at line 250 of file left_right.py.

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

Definition at line 249 of file left_right.py.

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

Definition at line 251 of file left_right.py.

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

Definition at line 252 of file left_right.py.

7.55.3.9 tuple rpki.left_right.bsc_elt.sql_template [static]

Initial value:

```
rpki.sql.template("bsc", "bsc_id", "self_id", "hash_alg",
                                   ("private_key_id", rpki.x509.RSA),
                                   ("pkcs10_request", rpki.x509.PKCS10),
                                   ("signing_cert", rpki.x509.X509),
                                   ("signing_cert_crl", rpki.x509.CRL))
```

Definition at line 243 of file left_right.py.

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

- left_right.py (1873)

7.56 rpki.left_right.child_elt Class Reference

Inheritance diagram for rpki.left_right.child_elt:

Public Member Functions

- def ca_from_class_name
- def child_certs
- def endElement
- def parents
- def serve_post_save_hook
- def serve_up_down

Static Public Attributes

- tuple attributes = ("action", "tag", "self_id", "child_id", "bsc_id")

  XML attributes for this element.

- tuple booleans = ("reissue",)

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

- bpki_cert = None
- bpki_glue = None
- clear_https_ta_cache = False
- string element_name = "child"
- tuple elements = ("bpki_cert", "bpki_glue")

  XML elements contained by this element.

- tuple sql_template

7.56.1 Detailed Description

```
<child/> element.
```

Definition at line 368 of file left_right.py.

7.56.2 Member Function Documentation

7.56.2.1 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 392 of file left_right.py.

7.56.2.2 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 384 of file left_right.py.

7.56.2.3 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 409 of file left_right.py.

7.56.2.4 def rpki.left_right.child_elt.parents (*self*)

```
Fetch all parent objects that link to self object to which this child object links.
```

Definition at line 388 of file left_right.py.

7.56.2.5 def rpki.left_right.child_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*)

```
Extra server actions for child_elt.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 402 of file left_right.py.

7.56.2.6 def rpki.left_right.child_elt.serve_up_down (*self*, *query*)

```
Outer layer of server handling for one up-down PDU from this child.
```

Definition at line 418 of file left_right.py.

7.56.3 Member Data Documentation

7.56.3.1 tuple rpki.left_right.child_elt.attributes = ("action", "tag", "self_id", "child_id", "bsc_id") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 372 of file left_right.py.

7.56.3.2 tuple rpki.left_right.child_elt.booleans = ("reissue",) [static]

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

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 374 of file left_right.py.

7.56.3.3 rpki.left_right.child_elt.bpki_cert = None [static]

Definition at line 380 of file left_right.py.

7.56.3.4 rpki.left_right.child_elt.bpki_glue = None [static]

Definition at line 381 of file left_right.py.

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

Definition at line 382 of file left_right.py.

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

Definition at line 371 of file left_right.py.

7.56.3.7 tuple rpki.left_right.child_elt.elements = ("bpki_cert", "bpki_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 373 of file left_right.py.

7.56.3.8 tuple rpki.left_right.child_elt.sql_template [static]

Initial value:

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

Definition at line 376 of file left_right.py.

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

- left_right.py (1873)

7.57 rpki.left_right.cms_msg Class Reference

Inheritance diagram for rpki.left_right.cms_msg:

Static Public Attributes

- string encoding = "us-ascii"
- saxify = sax_handler.saxify
- schema = rpki.relaxng.left_right

7.57.1 Detailed Description

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

Definition at line 813 of file left_right.py.

7.57.2 Member Data Documentation

7.57.2.1 string rpki.left_right.cms_msg.encoding = "us-ascii" [static]

Definition at line 816 of file left_right.py.

7.57.2.2 rpki.left_right.cms_msg.saxify = sax_handler.saxify [static]

Definition at line 818 of file left_right.py.

7.57.2.3 rpki.left_right.cms_msg.schema = rpki.relaxng.left_right [static]

Definition at line 817 of file left_right.py.

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

- left_right.py (1873)

7.58 rpki.left_right.data_elt Class Reference

Inheritance diagram for rpki.left_right.data_elt:

Public Member Functions

- def bsc
- def make_reply_clone_hook
- def self
- def serve_fetch_all
- def serve_fetch_one
- def unimplemented_control

7.58.1 Detailed Description

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

Definition at line 34 of file left_right.py.

7.58.2 Member Function Documentation

7.58.2.1 def rpki.left_right.data_elt.bsc (*self*)

```
Return BSC object to which this object links.
```

Definition at line 41 of file left_right.py.

7.58.2.2 def rpki.left_right.data_elt.make_reply_clone_hook (*self*, *r_pdu*)

```
Set self_id when cloning.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 45 of file left_right.py.

7.58.2.3 def rpki.left_right.data_elt.self (*this*)

```
Fetch self object to which this object links.
```

Definition at line 37 of file left_right.py.

7.58.2.4 def rpki.left_right.data_elt.serve_fetch_all (*self*)

```
Find the objects on which a list method should operate.
```

Reimplemented in rpki.left_right.self_elt.

Definition at line 60 of file left_right.py.

7.58.2.5 def rpki.left_right.data_elt.serve_fetch_one (*self*)

```
Find the object on which a get, set, or destroy method should
operate.
```

Reimplemented in rpki.left_right.self_elt.

Definition at line 49 of file left_right.py.

7.58.2.6 def rpki.left_right.data_elt.unimplemented_control (*self*, *controls*)

```
Uniform handling for unimplemented control operations.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 64 of file left_right.py.

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

- left_right.py (1873)

7.59 rpki.left_right.left_right_namespace Class Reference

Inheritance diagram for rpki.left_right.left_right_namespace:

Static Public Attributes

- dictionary nsmap = { None : xmlns }
- string xmlns = "http://www.hactrn.net/uris/rpki/left-right-spec/"

7.59.1 Detailed Description

`XML namespace parameters for left-right protocol.`

Definition at line 28 of file left_right.py.

7.59.2 Member Data Documentation

7.59.2.1 dictionary rpki.left_right.left_right_namespace.nsmap = { None : xmlns } [static]

Definition at line 32 of file left_right.py.

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

Definition at line 31 of file left_right.py.

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

- left_right.py (1873)

7.60 rpki.left_right.list_resources_elt Class Reference

Inheritance diagram for rpki.left_right.list_resources_elt:

Public Member Functions

- def startElement
- def toXML

Public Attributes

- asn
- ipv4
- ipv6

Static Public Attributes

- tuple attributes = ("self_id", "tag", "child_id", "valid_until", "asn", "ipv4", "ipv6", "subject_name")

  XML attributes for this element.

- string element_name = "list_resources"
- valid_until = None

7.60.1 Detailed Description

```
<list_resources/> element.
```

Definition at line 739 of file left_right.py.

7.60.2 Member Function Documentation

7.60.2.1 def rpki.left_right.list_resources_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle <list_resources/> element.  This requires special
handling due to the data types of some of the attributes.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 746 of file left_right.py.

7.60.2.2 def rpki.left_right.list_resources_elt.toXML (*self*)

```
Generate <list_resources/> element.  This requires special
handling due to the data types of some of the attributes.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 761 of file left_right.py.

7.60.3 Member Data Documentation

7.60.3.1 rpki.left_right.list_resources_elt.asn

Definition at line 755 of file left_right.py.

7.60.3.2 tuple rpki.left_right.list_resources_elt.attributes = ("self_id", "tag", "child_id", "valid_until", "asn", "ipv4", "ipv6", "subject_name") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 743 of file left_right.py.

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

Definition at line 742 of file left_right.py.

7.60.3.4 rpki.left_right.list_resources_elt.ipv4

Definition at line 757 of file left_right.py.

7.60.3.5 rpki.left_right.list_resources_elt.ipv6

Definition at line 759 of file left_right.py.

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

Definition at line 744 of file left_right.py.

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

- left_right.py (1873)

7.61 rpki.left_right.msg Class Reference

Inheritance diagram for rpki.left_right.msg:

Public Member Functions

- def serve_top_level

Static Public Attributes

- tuple pdus

  Dispatch table of PDUs for this protocol.

- int version = 1

  Protocol version.

7.61.1 Detailed Description

```
Left-right PDU.
```

Definition at line 784 of file left_right.py.

7.61.2 Member Function Documentation

7.61.2.1 def rpki.left_right.msg.serve_top_level (*self*, *gctx*)

```
Serve one msg PDU.
```

Definition at line 797 of file left_right.py.

7.61.3 Member Data Documentation

7.61.3.1 rpki::left_right.msg::pdus [static]

Initial value:

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

Dispatch table of PDUs for this protocol.

Definition at line 793 of file left_right.py.

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

Protocol version.

Reimplemented from rpki.xml_utils.msg.

Definition at line 789 of file left_right.py.

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

- left_right.py (1873)

7.62 rpki.left_right.parent_elt Class Reference

Inheritance diagram for rpki.left_right.parent_elt:

Public Member Functions

- def cas
- def query_up_down
- def repository
- def serve_post_save_hook
- def serve_rekey
- def serve_revoke

Static Public Attributes

- tuple attributes

  XML attributes for this element.

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

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

- bpki_cms_cert = None
- bpki_cms_glue = None
- bpki_https_cert = None
- bpki_https_glue = None
- string element_name = "parent"
- tuple elements = ("bpki_cms_cert", "bpki_cms_glue", "bpki_https_cert", "bpki_https_glue")

  XML elements contained by this element.

- tuple sql_template

7.62.1 Detailed Description

```
<parent/> element.
```

Definition at line 278 of file left_right.py.

7.62.2 Member Function Documentation

7.62.2.1 def rpki.left_right.parent_elt.cas (*self*)

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

Definition at line 301 of file left_right.py.

7.62.2.2 def rpki.left_right.parent_elt.query_up_down (*self*, *q_pdu*)

```
Client code for sending one up-down query PDU to this parent.

I haven't figured out yet whether this method should do something
clever like dispatching via a method in the response PDU payload,
or just hand back the whole response to the caller.  In the long
run this will have to become event driven with a context object
that has methods of its own, but as this method is common code for
several different queries and I don't yet know what the response
processing looks like, it's too soon to tell what will make sense.

For now, keep this dead simple lock step, rewrite it later.
```

Definition at line 323 of file left_right.py.

7.62.2.3 def rpki.left_right.parent_elt.repository (*self*)

```
Fetch repository object to which this parent object links.
```

Definition at line 297 of file left_right.py.

7.62.2.4 def rpki.left_right.parent_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*)

```
Extra server actions for parent_elt.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 305 of file left_right.py.

7.62.2.5 def rpki.left_right.parent_elt.serve_rekey (*self*)

```
Handle a left-right rekey action for this parent.
```

Definition at line 313 of file left_right.py.

7.62.2.6 def rpki.left_right.parent_elt.serve_revoke (*self*)

```
Handle a left-right revoke action for this parent.
```

Definition at line 318 of file left_right.py.

7.62.3 Member Data Documentation

7.62.3.1 tuple rpki.left_right.parent_elt.attributes [static]

Initial value:

```
("action", "tag", "self_id", "parent_id", "bsc_id", "repository_id",
                "peer_contact_uri", "sia_base", "sender_name", "recipient_name")
```

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 282 of file left_right.py.

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

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

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 285 of file left_right.py.

7.62.3.3 rpki.left_right.parent_elt.bpki_cms_cert = None [static]

Definition at line 292 of file left_right.py.

7.62.3.4 rpki.left_right.parent_elt.bpki_cms_glue = None [static]

Definition at line 293 of file left_right.py.

7.62.3.5 rpki.left_right.parent_elt.bpki_https_cert = None [static]

Definition at line 294 of file left_right.py.

7.62.3.6 rpki.left_right.parent_elt.bpki_https_glue = None [static]

Definition at line 295 of file left_right.py.

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

Definition at line 281 of file left_right.py.

7.62.3.8 tuple rpki.left_right.parent_elt.elements = ("bpki_cms_cert", "bpki_cms_glue", "bpki_https_cert", "bpki_https_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 284 of file left_right.py.

7.62.3.9 tuple rpki.left_right.parent_elt.sql_template [static]

Initial value:

```
rpki.sql.template("parent", "parent_id", "self_id", "bsc_id", "repository_id",
                                  ("bpki_cms_cert", rpki.x509.X509), ("bpki_cms_glue", rpki.x509.X5
                                  ("bpki_https_cert", rpki.x509.X509), ("bpki_https_glue", rpki.x50
                                  "peer_contact_uri", "sia_base", "sender_name", "recipient_name")
```

Definition at line 287 of file left_right.py.

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

- left_right.py (1873)

7.63 rpki.left_right.report_error_elt Class Reference

Inheritance diagram for rpki.left_right.report_error_elt:

Public Member Functions

- def from_exception

Public Attributes

- error_code
- self_id

Static Public Attributes

- tuple attributes = ("tag", "self_id", "error_code")

  XML attributes for this element.

- string element_name = "report_error"

7.63.1 Detailed Description

```
<report_error/> element.
```

Definition at line 770 of file left_right.py.

7.63.2 Member Function Documentation

7.63.2.1 def rpki.left_right.report_error_elt.from_exception (*cls*, *exc*, *self_id* = None)

```
Generate a <report_error/> element from an exception.
```

Definition at line 777 of file left_right.py.

7.63.3 Member Data Documentation

7.63.3.1 tuple rpki.left_right.report_error_elt.attributes = ("tag", "self_id", "error_code") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 774 of file left_right.py.

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

Definition at line 773 of file left_right.py.

7.63.3.3 rpki.left_right.report_error_elt.error_code

Definition at line 781 of file left_right.py.

7.63.3.4 rpki.left_right.report_error_elt.self_id

Definition at line 780 of file left_right.py.

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

- left_right.py (1873)

7.64 rpki.left_right.repository_elt Class Reference

Inheritance diagram for rpki.left_right.repository_elt:

Public Member Functions

- def call_pubd
- def object_delete
- def object_write
- def parents
- def publish
- def uri_to_filename
- def withdraw

Static Public Attributes

- tuple attributes = ("action", "tag", "self_id", "repository_id", "bsc_id", "peer_-contact_uri")

  XML attributes for this element.

- bpki_cms_cert = None
- bpki_cms_glue = None
- bpki_https_cert = None
- bpki_https_glue = None
- string element_name = "repository"
- tuple elements = ("bpki_cms_cert", "bpki_cms_glue", "bpki_https_cert", "bpki_https_glue")

  XML elements contained by this element.

- tuple sql_template
- use_pubd = True

7.64.1 Detailed Description

```
<repository/> element.
```

Definition at line 446 of file left_right.py.

7.64.2 Member Function Documentation

7.64.2.1 def rpki.left_right.repository_elt.call_pubd (*self*, *pdus*)

```
Send a message to publication daemon and return the response.
```

Definition at line 496 of file left_right.py.

7.64.2.2 def rpki.left_right.repository_elt.object_delete (*cls*, *base*, *uri*)

```
Delete an object from disk. [TEMPORARY]
```

Definition at line 491 of file left_right.py.

7.64.2.3 def rpki.left_right.repository_elt.object_write (*cls*, *base*, *uri*, *obj*)

```
Write an object to disk. [TEMPORARY]
```

Definition at line 479 of file left_right.py.

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

```
Fetch all parent objects that link to this repository object.
```

Definition at line 464 of file left_right.py.

7.64.2.5 def rpki.left_right.repository_elt.publish (*self*, *obj*, *uri*)

```
Placeholder for publication operation. [TEMPORARY]
```

Definition at line 514 of file left_right.py.

7.64.2.6 def rpki.left_right.repository_elt.uri_to_filename (*base*, *uri*)

```
Convert a URI to a filename. [TEMPORARY]
```

Definition at line 469 of file left_right.py.

7.64.2.7 def rpki.left_right.repository_elt.withdraw (*self*, *obj*, *uri*)

```
Placeholder for publication withdrawal operation. [TEMPORARY]
```

Definition at line 523 of file left_right.py.

7.64.3 Member Data Documentation

7.64.3.1 tuple rpki.left_right.repository_elt.attributes = ("action", "tag", "self_-id", "repository_id", "bsc_id", "peer_contact_uri") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 450 of file left_right.py.

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

Definition at line 457 of file left_right.py.

7.64.3.3 rpki.left_right.repository_elt.bpki_cms_glue = None [static]

Definition at line 458 of file left_right.py.

7.64.3.4 rpki.left_right.repository_elt.bpki_https_cert = None [static]

Definition at line 459 of file left_right.py.

7.64.3.5 rpki.left_right.repository_elt.bpki_https_glue = None [static]

Definition at line 460 of file left_right.py.

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

Definition at line 449 of file left_right.py.

7.64.3.7 tuple rpki.left_right.repository_elt.elements = ("bpki_cms_cert", "bpki_cms_glue", "bpki_https_cert", "bpki_https_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 451 of file left_right.py.

7.64.3.8 tuple rpki.left_right.repository_elt.sql_template [static]

Initial value:

```
rpki.sql.template("repository", "repository_id", "self_id", "bsc_id", "peer_contact_uri",
                                  ("bpki_cms_cert", rpki.x509.X509), ("bpki_cms_glue", rpki.x509.X5
                                  ("bpki_https_cert", rpki.x509.X509), ("bpki_https_glue", rpki.x50
```

Definition at line 453 of file left_right.py.

7.64.3.9 rpki.left_right.repository_elt.use_pubd = True [static]

Definition at line 462 of file left_right.py.

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

- left_right.py (1873)

7.65 rpki.left_right.route_origin_elt Class Reference

Inheritance diagram for rpki.left_right.route_origin_elt:

Public Member Functions

- def ca_detail
- def ee_uri
- def ee_uri_tail
- def generate_roa
- def regenerate_roa
- def roa_uri
- def serve_post_save_hook
- def sql_delete_hook
- def sql_fetch_hook
- def sql_insert_hook
- def startElement
- def update_roa
- def withdraw_roa

Public Attributes

- as_number
- ipv4
- ipv6

Static Public Attributes

- tuple attributes = ("action", "tag", "self_id", "route_origin_id", "as_number", "ipv4", "ipv6")

  XML attributes for this element.

- tuple booleans = ("suppress_publication",)

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

- ca_detail_id = None
- cert = None
- string element_name = "route_origin"
- roa = None
- tuple sql_template

7.65.1 Detailed Description

`<route_origin/> element.`

Definition at line 532 of file left_right.py.

7.65.2 Member Function Documentation

7.65.2.1 def rpki.left_right.route_origin_elt.ca_detail (*self*)

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

Definition at line 576 of file left_right.py.

7.65.2.2 def rpki.left_right.route_origin_elt.ee_uri (*self*, *ca*)

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

Definition at line 735 of file left_right.py.

7.65.2.3 def rpki.left_right.route_origin_elt.ee_uri_tail (*self*)

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

Definition at line 731 of file left_right.py.

7.65.2.4 def rpki.left_right.route_origin_elt.generate_roa (*self*)

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

At present this does not support ROAs with multiple signatures
(neither does the current CMS code).

At present we have no way of performing a direct lookup from a
desired set of resources to a covering certificate, so we have to
search.  This could be quite slow if we have a lot of active
ca_detail objects.  Punt on the issue for now, revisit if
profiling shows this as a hotspot.

Once we have the right covering certificate, we generate the ROA
payload, generate a new EE certificate, use the EE certificate to
sign the ROA payload, publish the result, then throw away the
private key for the EE cert, all per the ROA specification.  This
implies that generating a lot of ROAs will tend to thrash
/dev/random, but there is not much we can do about that.
```

Definition at line 625 of file left_right.py.

7.65.2.5 def rpki.left_right.route_origin_elt.regenerate_roa (*self*)

```
Reissue ROA associated with this route_origin.
```

Definition at line 723 of file left_right.py.

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

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

Definition at line 727 of file left_right.py.

7.65.2.7 def rpki.left_right.route_origin_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*)

```
Extra server actions for route_origin_elt.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 580 of file left_right.py.

7.65.2.8 def rpki.left_right.route_origin_elt.sql_delete_hook (*self*)

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

Reimplemented from rpki.sql.sql_persistant.

Definition at line 572 of file left_right.py.

7.65.2.9 def rpki.left_right.route_origin_elt.sql_fetch_hook (*self*)

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

Reimplemented from rpki.sql.sql_persistant.

Definition at line 548 of file left_right.py.

7.65.2.10 def rpki.left_right.route_origin_elt.sql_insert_hook (*self*)

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

Reimplemented from rpki.sql.sql_persistant.

Definition at line 563 of file left_right.py.

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

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

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 584 of file left_right.py.

7.65.2.12 def rpki.left_right.route_origin_elt.update_roa (*self*)

```
Bring this route_origin's ROA up to date if necesssary.
```

Definition at line 597 of file left_right.py.

7.65.2.13 def rpki.left_right.route_origin_elt.withdraw_roa (*self*, *regenerate* = `False`)

```
Withdraw ROA associated with this route_origin.

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

Definition at line 694 of file left_right.py.

7.65.3 Member Data Documentation

7.65.3.1 rpki.left_right.route_origin_elt.as_number

Definition at line 591 of file left_right.py.

7.65.3.2 tuple rpki.left_right.route_origin_elt.attributes = ("action", "tag", "self_id", "route_origin_id", "as_number", "ipv4", "ipv6") `[static]`

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 536 of file left_right.py.

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

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

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 537 of file left_right.py.

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

Definition at line 544 of file left_right.py.

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

Definition at line 545 of file left_right.py.

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

Definition at line 535 of file left_right.py.

7.65.3.7 rpki.left_right.route_origin_elt.ipv4

Definition at line 550 of file left_right.py.

7.65.3.8 rpki.left_right.route_origin_elt.ipv6

Definition at line 556 of file left_right.py.

7.65.3.9 rpki.left_right.route_origin_elt.roa = None [static]

Definition at line 546 of file left_right.py.

7.65.3.10 tuple rpki.left_right.route_origin_elt.sql_template [static]

Initial value:

```
rpki.sql.template("route_origin", "route_origin_id", "ca_detail_id",
                                  "self_id", "as_number",
                                  ("roa", rpki.x509.ROA),
                                  ("cert", rpki.x509.X509))
```

Definition at line 539 of file left_right.py.

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

- left_right.py (1873)

7.66 rpki.left_right.sax_handler Class Reference

Inheritance diagram for rpki.left_right.sax_handler:

Static Public Attributes

- string name = "msg"
- pdu = msg
- string version = "1"

7.66.1 Detailed Description

`SAX handler for Left-Right protocol.`

Definition at line 806 of file left_right.py.

7.66.2 Member Data Documentation

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

Definition at line 810 of file left_right.py.

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

Definition at line 809 of file left_right.py.

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

Definition at line 811 of file left_right.py.

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

- left_right.py (1873)

7.67 rpki.left_right.self_elt Class Reference

Inheritance diagram for rpki.left_right.self_elt:

Public Member Functions

- def bscs
- def children
- def client_poll
- def parents
- def regenerate_crls_and_manifests
- def repositories
- def route_origins
- def serve_fetch_all
- def serve_fetch_one
- def serve_post_save_hook
- def serve_rekey
- def serve_revoke
- def update_children
- def update_roas

Static Public Attributes

- tuple attributes = ("action", "tag", "self_id", "crl_interval", "regen_margin")

  XML attributes for this element.

- tuple booleans = ("rekey", "reissue", "revoke", "run_now", "publish_world_now")

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

- bpki_cert = None
- bpki_glue = None
- crl_interval = None
- string element_name = "self"
- tuple elements = ("bpki_cert", "bpki_glue")

  XML elements contained by this element.

- regen_margin = None
- self_id = None
- tuple sql_template
- use_hsm = False

7.67.1 Detailed Description

`<self/> element.`

Definition at line 70 of file left_right.py.

7.67.2 Member Function Documentation

7.67.2.1 def rpki.left_right.self_elt.bscs (*self*)

```
Fetch all BSC objects that link to this self object.
```

Definition at line 88 of file left_right.py.

7.67.2.2 def rpki.left_right.self_elt.children (*self*)

```
Fetch all child objects that link to this self object.
```

Definition at line 100 of file left_right.py.

7.67.2.3 def rpki.left_right.self_elt.client_poll (*self*)

```
Run the regular client poll cycle with each of this self's parents in turn.
```

Definition at line 145 of file left_right.py.

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

```
Fetch all parent objects that link to this self object.
```

Definition at line 96 of file left_right.py.

7.67.2.5 def rpki.left_right.self_elt.regenerate_crls_and_manifests (*self*)

```
Generate new CRLs and manifests as necessary for all of this
self's CAs.  Extracting nextUpdate from a manifest is hard at the
moment due to implementation silliness, so for now we generate a
new manifest whenever we generate a new CRL

This method also cleans up tombstones left behind by revoked
ca_detail objects, since we're walking through the relevant
portions of the database anyway.
```

Definition at line 204 of file left_right.py.

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

```
Fetch all repository objects that link to this self object.
```

Definition at line 92 of file left_right.py.

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

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

Definition at line 104 of file left_right.py.

7.67.2.8 def rpki.left_right.self_elt.serve_fetch_all (*self*)

```
Find the self objects upon which a list action should operate.
This is different from the list action for all other objects,
where list only works within a given self_id context.
```

Reimplemented from rpki.left_right.data_elt.

Definition at line 138 of file left_right.py.

7.67.2.9 def rpki.left_right.self_elt.serve_fetch_one (*self*)

```
Find the self object upon which a get, set, or destroy action
should operate.
```

Reimplemented from rpki.left_right.data_elt.

Definition at line 129 of file left_right.py.

7.67.2.10 def rpki.left_right.self_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*)

```
Extra server actions for self_elt.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 108 of file left_right.py.

7.67.2.11 def rpki.left_right.self_elt.serve_rekey (*self*)

```
Handle a left-right rekey action for this self.
```

Definition at line 117 of file left_right.py.

7.67.2.12 def rpki.left_right.self_elt.serve_revoke (*self*)

```
Handle a left-right revoke action for this self.
```

Definition at line 123 of file left_right.py.

7.67.2.13 def rpki.left_right.self_elt.update_children (*self*)

```
Check for updated IRDB data for all of this self's children and
issue new certs as necessary.  Must handle changes both in
resources and in expiration date.
```

Definition at line 167 of file left_right.py.

7.67.2.14 def rpki.left_right.self_elt.update_roas (*self*)

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

Definition at line 229 of file left_right.py.

7.67.3 Member Data Documentation

7.67.3.1 tuple rpki.left_right.self_elt.attributes = ("action", "tag", "self_id", "crl_interval", "regen_margin") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 74 of file left_right.py.

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

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

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 76 of file left_right.py.

7.67.3.3 rpki.left_right.self_elt.bpki_cert = None [static]

Definition at line 85 of file left_right.py.

7.67.3.4 rpki.left_right.self_elt.bpki_glue = None [static]

Definition at line 86 of file left_right.py.

7.67.3.5 rpki.left_right.self_elt.crl_interval = None [static]

Definition at line 83 of file left_right.py.

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

Definition at line 73 of file left_right.py.

7.67.3.7 tuple rpki.left_right.self_elt.elements = ("bpki_cert", "bpki_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 75 of file left_right.py.

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

Definition at line 84 of file left_right.py.

7.67.3.9 rpki.left_right.self_elt.self_id = None [static]

Definition at line 81 of file left_right.py.

7.67.3.10 tuple rpki.left_right.self_elt.sql_template [static]

Initial value:

```
rpki.sql.template("self", "self_id", "use_hsm", "crl_interval", "regen_margin",
                                  ("bpki_cert", rpki.x509.X509), ("bpki_glue", rpki.x509.X509))
```

Definition at line 78 of file left_right.py.

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

Definition at line 82 of file left_right.py.

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

- left_right.py (1873)

7.68 rpki.log.logger Class Reference

Inheritance diagram for rpki.log.logger:

Public Member Functions

- def __call__
- def __init__

Public Attributes

- priority

7.68.1 Detailed Description

```
Closure for logging.
```

Definition at line 38 of file log.py.

7.68.2 Member Function Documentation

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

Definition at line 44 of file log.py.

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

Definition at line 41 of file log.py.

7.68.3 Member Data Documentation

7.68.3.1 rpki.log.logger.priority

Definition at line 42 of file log.py.

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

- log.py (1873)

7.69 rpki.manifest.FileAndHash Class Reference

Inheritance diagram for rpki.manifest.FileAndHash:

Public Member Functions

- def __init__

Public Attributes

- file
- hash

7.69.1 Detailed Description

Definition at line 26 of file manifest.py.

7.69.2 Member Function Documentation

7.69.2.1 def rpki.manifest.FileAndHash.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 27 of file manifest.py.

7.69.3 Member Data Documentation

7.69.3.1 rpki.manifest.FileAndHash.file

Definition at line 28 of file manifest.py.

7.69.3.2 rpki.manifest.FileAndHash.hash

Definition at line 29 of file manifest.py.

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

- manifest.py (1873)

7.70 rpki.manifest.FilesAndHashes Class Reference

Inheritance diagram for rpki.manifest.FilesAndHashes:

Public Member Functions

- def __init__

7.70.1 Detailed Description

Definition at line 33 of file manifest.py.

7.70.2 Member Function Documentation

7.70.2.1 def rpki.manifest.FilesAndHashes.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 34 of file manifest.py.

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

- manifest.py (1873)

7.71 rpki.manifest.Manifest Class Reference

Inheritance diagram for rpki.manifest.Manifest:

Public Member Functions

- def __init__

Public Attributes

- explicitVersion
- fileHashAlg
- fileList
- manifestNumber
- nextUpdate
- thisUpdate
- version

7.71.1 Detailed Description

Definition at line 37 of file manifest.py.

7.71.2 Member Function Documentation

7.71.2.1 def rpki.manifest.Manifest.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 38 of file manifest.py.

7.71.3 Member Data Documentation

7.71.3.1 rpki.manifest.Manifest.explicitVersion

Definition at line 40 of file manifest.py.

7.71.3.2 rpki.manifest.Manifest.fileHashAlg

Definition at line 44 of file manifest.py.

7.71.3.3 rpki.manifest.Manifest.fileList

Definition at line 45 of file manifest.py.

7.71.3.4 rpki.manifest.Manifest.manifestNumber

Definition at line 41 of file manifest.py.

7.71.3.5 rpki.manifest.Manifest.nextUpdate

Definition at line 43 of file manifest.py.

7.71.3.6 rpki.manifest.Manifest.thisUpdate

Definition at line 42 of file manifest.py.

7.71.3.7 rpki.manifest.Manifest.version

Definition at line 39 of file manifest.py.

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

- manifest.py (1873)

7.72 rpki.publication.certificate_elt Class Reference

Inheritance diagram for rpki.publication.certificate_elt:

Static Public Attributes

- string element_name = "certificate"
- payload_type = rpki.x509.X509

7.72.1 Detailed Description

`<certificate/> element.`

Definition at line 205 of file publication.py.

7.72.2 Member Data Documentation

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

Definition at line 208 of file publication.py.

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

Definition at line 209 of file publication.py.

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

- publication.py (1873)

7.73 rpki.publication.client_elt Class Reference

Inheritance diagram for rpki.publication.client_elt:

Public Member Functions

- def check_allowed_uri
- def endElement
- def serve_fetch_all
- def serve_fetch_one
- def serve_post_save_hook

Static Public Attributes

- tuple attributes = ("action", "tag", "client_id", "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", "base_uri", ("bpki_-cert", rpki.x509.X509), ("bpki_glue", rpki.x509.X509))

7.73.1 Detailed Description

```
<client/> element.
```

Definition at line 91 of file publication.py.

7.73.2 Member Function Documentation

7.73.2.1 def rpki.publication.client_elt.check_allowed_uri (*self*, *uri*)

Definition at line 134 of file publication.py.

7.73.2.2 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 106 of file publication.py.

7.73.2.3 def rpki.publication.client_elt.serve_fetch_all (*self*)

```
Find client objects on which a list method should operate.
```

Definition at line 130 of file publication.py.

7.73.2.4 def rpki.publication.client_elt.serve_fetch_one (*self*)

```
Find the client object on which a get, set, or destroy method
should operate.
```

Definition at line 121 of file publication.py.

7.73.2.5 def rpki.publication.client_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*)

```
Extra server actions for client_elt.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 115 of file publication.py.

7.73.3 Member Data Documentation

7.73.3.1 tuple rpki.publication.client_elt.attributes = ("action", "tag", "client_id", "base_uri") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 95 of file publication.py.

7.73.3.2 rpki.publication.client_elt.base_uri = None [static]

Definition at line 100 of file publication.py.

7.73.3.3 rpki.publication.client_elt.bpki_cert = None [static]

Definition at line 101 of file publication.py.

7.73.3.4 rpki.publication.client_elt.bpki_glue = None [static]

Definition at line 102 of file publication.py.

7.73.3.5 rpki.publication.client_elt.clear_https_ta_cache = False [static]

Definition at line 104 of file publication.py.

7.73.3.6 string rpki.publication.client_elt.element_name = "client" [static]

Definition at line 94 of file publication.py.

7.73.3.7 tuple rpki.publication.client_elt.elements = ("bpki_cert", "bpki_glue") [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 96 of file publication.py.

7.73.3.8 tuple rpki.publication.client_elt.sql_template = rpki.sql.template("client", "client_id", "base_uri", ("bpki_cert", rpki.x509.X509), ("bpki_glue", rpki.x509.X509)) [static]

Definition at line 98 of file publication.py.

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

- publication.py (1873)

7.74 rpki.publication.cms_msg Class Reference

Inheritance diagram for rpki.publication.cms_msg:

Static Public Attributes

- string encoding = "us-ascii"
- saxify = sax_handler.saxify
- schema = rpki.relaxng.publication

7.74.1 Detailed Description

`Class to hold a CMS-signed publication PDU.`

Definition at line 277 of file publication.py.

7.74.2 Member Data Documentation

7.74.2.1 string rpki.publication.cms_msg.encoding = "us-ascii" [static]

Definition at line 280 of file publication.py.

7.74.2.2 rpki.publication.cms_msg.saxify = sax_handler.saxify [static]

Definition at line 282 of file publication.py.

7.74.2.3 rpki.publication.cms_msg.schema = rpki.relaxng.publication [static]

Definition at line 281 of file publication.py.

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

- publication.py (1873)

7.75 rpki.publication.config_elt Class Reference

Inheritance diagram for rpki.publication.config_elt:

Public Member Functions

- def fetch
- def serve_fetch_one
- def serve_set
- def startElement

Public Attributes

- config_id

Static Public Attributes

- tuple attributes = ("action", "tag")

  XML attributes for this element.

- string element_name = "config"
- tuple elements = ("bpki_crl",)

  XML elements contained by this element.

- tuple sql_template = rpki.sql.template("config", "config_id", ("bpki_crl", rpki.x509.CRL))
- int wired_in_config_id = 1

7.75.1 Detailed Description

```
<config/> element.  This is a little weird because there should
never be more than one row in the SQL config table, but we have to
put the BPKI CRL somewhere and SQL is the least bad place available.

So we reuse a lot of the SQL machinery, but we nail config_id at 1,
we don't expose it in the XML protocol, and we only support the get
and set actions.
```

Definition at line 41 of file publication.py.

7.75.2 Member Function Documentation

7.75.2.1 def rpki.publication.config_elt.fetch (*cls*, *gctx*)

```
Fetch the config object from SQL.  This requires special
handling because of the weird way we treat config_id.
```

Definition at line 67 of file publication.py.

7.75.2.2 def rpki.publication.config_elt.serve_fetch_one (*self*)

```
Find the config object on which a get or set method should
operate.
```

Definition at line 82 of file publication.py.

7.75.2.3 def rpki.publication.config_elt.serve_set (*self*, *r_msg*)

```
Handle a set action.  This requires special handling because
config we don't support the create method.
```

Reimplemented from rpki.xml_utils.data_elt.

Definition at line 73 of file publication.py.

7.75.2.4 def rpki.publication.config_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
StartElement() handler for config object.  This requires
special handling because of the weird way we treat config_id.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 59 of file publication.py.

7.75.3 Member Data Documentation

7.75.3.1 tuple rpki.publication.config_elt.attributes = ("action", "tag") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 51 of file publication.py.

7.75.3.2 rpki.publication.config_elt.config_id

Definition at line 64 of file publication.py.

7.75.3.3 string rpki.publication.config_elt.element_name = "config" [static]

Definition at line 52 of file publication.py.

7.75.3.4 tuple rpki.publication.config_elt.elements = ("bpki_crl",) [static]

XML elements contained by this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 53 of file publication.py.

7.75.3.5 tuple rpki.publication.config_elt.sql_template = rpki.sql.template("config", "config_id", ("bpki_crl", rpki.x509.CRL)) [static]

Definition at line 55 of file publication.py.

7.75.3.6 int rpki.publication.config_elt.wired_in_config_id = 1 [static]

Definition at line 57 of file publication.py.

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

- publication.py (1873)

7.76 rpki.publication.control_elt Class Reference

Inheritance diagram for rpki.publication.control_elt:

Public Member Functions

- def serve_dispatch

7.76.1 Detailed Description

```
Virtual class for control channel objects.
```

Definition at line 30 of file publication.py.

7.76.2 Member Function Documentation

7.76.2.1 def rpki.publication.control_elt.serve_dispatch (*self*, *r_msg*, *client*)

```
Action dispatch handler.  This needs special handling because
we need to make sure that this PDU arrived via the control channel.
```

Definition at line 33 of file publication.py.

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

- publication.py (1873)

7.77 rpki.publication.crl_elt Class Reference

Inheritance diagram for rpki.publication.crl_elt:

Static Public Attributes

- string element_name = "crl"
- payload_type = rpki.x509.CRL

7.77.1 Detailed Description

`<crl/> element.`

Definition at line 211 of file publication.py.

7.77.2 Member Data Documentation

7.77.2.1 string rpki.publication.crl_elt.element_name = "crl" [static]

Definition at line 214 of file publication.py.

7.77.2.2 rpki.publication.crl_elt.payload_type = rpki.x509.CRL [static]

Definition at line 215 of file publication.py.

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

- publication.py (1873)

7.78 rpki.publication.manifest_elt Class Reference

Inheritance diagram for rpki.publication.manifest_elt:

Static Public Attributes

- string element_name = "manifest"
- payload_type = rpki.x509.SignedManifest

7.78.1 Detailed Description

`<manifest/> element.`

Definition at line 217 of file publication.py.

7.78.2 Member Data Documentation

7.78.2.1 string rpki.publication.manifest_elt.element_name = "manifest" [static]

Definition at line 220 of file publication.py.

7.78.2.2 rpki.publication.manifest_elt.payload_type = rpki.x509.SignedManifest [static]

Definition at line 221 of file publication.py.

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

- publication.py (1873)

7.79 rpki.publication.msg Class Reference

Inheritance diagram for rpki.publication.msg:

Public Member Functions

- def serve_top_level

Static Public Attributes

- tuple pdus

  Dispatch table of PDUs for this protocol.

- int version = 1

  Protocol version.

7.79.1 Detailed Description

```
Publication PDU.
```

Definition at line 247 of file publication.py.

7.79.2 Member Function Documentation

7.79.2.1 def rpki.publication.msg.serve_top_level (*self*, *gctx*, *client*)

```
Serve one msg PDU.
```

Definition at line 259 of file publication.py.

7.79.3 Member Data Documentation

7.79.3.1 rpki::publication.msg::pdus [static]

Initial value:

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

Dispatch table of PDUs for this protocol.

Definition at line 256 of file publication.py.

7.79.3.2 rpki::publication.msg::version = 1 [static]

Protocol version.

Reimplemented from rpki.xml_utils.msg.

Definition at line 252 of file publication.py.

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

- publication.py (1873)

7.80 rpki.publication.publication_namespace Class Reference

Inheritance diagram for rpki.publication.publication_namespace:

Static Public Attributes

- dictionary nsmap = { None : xmlns }
- string xmlns = "http://www.hactrn.net/uris/rpki/publication-spec/"

7.80.1 Detailed Description

`XML namespace parameters for publication protocol.`

Definition at line 24 of file publication.py.

7.80.2 Member Data Documentation

7.80.2.1 dictionary rpki.publication.publication_namespace.nsmap = { None : xmlns } [static]

Definition at line 28 of file publication.py.

7.80.2.2 string rpki.publication.publication_namespace.xmlns = "http://www.hactrn.net/uris/rpki/publication-spec/" [static]

Definition at line 27 of file publication.py.

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

- publication.py (1873)

7.81 rpki.publication.publication_object_elt Class Reference

Inheritance diagram for rpki.publication.publication_object_elt:

Public Member Functions

- def endElement
- def serve_dispatch
- def serve_publish
- def serve_withdraw
- def toXML

- def uri_to_filename

Static Public Attributes

- tuple attributes = ("action", "tag", "client_id", "uri")

  XML attributes for this element.

- payload = None

7.81.1 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 138 of file publication.py.

7.81.2 Member Function Documentation

7.81.2.1 def rpki.publication.publication_object_elt.endElement (*self*, *stack*, *name*, *text*)

```
Handle a publishable element element.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 150 of file publication.py.

7.81.2.2 def rpki.publication.publication_object_elt.serve_dispatch (*self*, *r_msg*, *client*)

```
Action dispatch handler.
```

Definition at line 164 of file publication.py.

7.81.2.3 def rpki.publication.publication_object_elt.serve_publish (*self*)

```
Publish an object.
```

Definition at line 180 of file publication.py.

7.81.2.4 def rpki.publication.publication_object_elt.serve_withdraw (*self*)

```
Withdraw an object.
```

Definition at line 191 of file publication.py.

7.81.2.5 def rpki.publication.publication_object_elt.toXML (*self*)

```
Generate XML element for publishable object.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 157 of file publication.py.

7.81.2.6 def rpki.publication.publication_object_elt.uri_to_filename (*self*)

```
Convert a URI to a local filename.
```

Definition at line 196 of file publication.py.

7.81.3 Member Data Documentation

7.81.3.1 tuple rpki.publication.publication_object_elt.attributes = ("action", "tag", "client_id", "uri") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 147 of file publication.py.

7.81.3.2 rpki.publication.publication_object_elt.payload = None [static]

Definition at line 148 of file publication.py.

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

- publication.py (1873)

7.82 rpki.publication.report_error_elt Class Reference

Inheritance diagram for rpki.publication.report_error_elt:

Public Member Functions

- def from_exception

Public Attributes

- error_code

Static Public Attributes

- tuple attributes = ("tag", "error_code")

  XML attributes for this element.

- string element_name = "report_error"

7.82.1 Detailed Description

```
<report_error/> element.
```

Definition at line 234 of file publication.py.

7.82.2 Member Function Documentation

7.82.2.1 def rpki.publication.report_error_elt.from_exception (*cls*, *exc*)

```
Generate a <report_error/> element from an exception.
```

Definition at line 241 of file publication.py.

7.82.3 Member Data Documentation

7.82.3.1 tuple rpki.publication.report_error_elt.attributes = ("tag", "error_code") [static]

XML attributes for this element.

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 238 of file publication.py.

7.82.3.2 string rpki.publication.report_error_elt.element_name = "report_error" [static]

Definition at line 237 of file publication.py.

7.82.3.3 rpki.publication.report_error_elt.error_code

Definition at line 244 of file publication.py.

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

- publication.py (1873)

7.83 rpki.publication.roa_elt Class Reference

Inheritance diagram for rpki.publication.roa_elt:

Static Public Attributes

- string element_name = "roa"
- payload_type = rpki.x509.ROA

7.83.1 Detailed Description

`<roa/> element.`

Definition at line 223 of file publication.py.

7.83.2 Member Data Documentation

7.83.2.1 string rpki.publication.roa_elt.element_name = "roa" [static]

Definition at line 226 of file publication.py.

7.83.2.2 rpki.publication.roa_elt.payload_type = rpki.x509.ROA [static]

Definition at line 227 of file publication.py.

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

- publication.py (1873)

7.84 rpki.publication.sax_handler Class Reference

Inheritance diagram for rpki.publication.sax_handler:

Static Public Attributes

- string name = "msg"
- pdu = msg
- string version = "1"

7.84.1 Detailed Description

`SAX handler for publication protocol.`

Definition at line 270 of file publication.py.

7.84.2 Member Data Documentation

7.84.2.1 string rpki.publication.sax_handler.name = "msg" [static]

Definition at line 274 of file publication.py.

7.84.2.2 rpki.publication.sax_handler.pdu = msg [static]

Definition at line 273 of file publication.py.

7.84.2.3 string rpki.publication.sax_handler.version = "1" [static]

Definition at line 275 of file publication.py.

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

- publication.py (1873)

7.85 rpki.resource_set.resource_bag Class Reference

Inheritance diagram for rpki.resource_set.resource_bag:

Public Member Functions

- def __eq__
- def __init__
- def __ne__
- def __str__
- def empty
- def from_rfc3779_tuples
- def intersection
- def oversized
- def undersized
- def union

Public Attributes

- asn

  Set of Autonomous System Number resources.

- v4

  Set of IPv4 resources.

- v6

  Set of IPv6 resources.

- valid_until

  Expiration date of resources, for setting certificate notAfter field.

7.85.1 Detailed Description

```
Container to simplify passing around the usual triple of ASN,
IPv4, and IPv6 resource sets.
```

Definition at line 448 of file resource_set.py.

7.85.2 Member Function Documentation

7.85.2.1 def rpki.resource_set.resource_bag.__eq__ (*self*, *other*)

Definition at line 508 of file resource_set.py.

7.85.2.2 def rpki.resource_set.resource_bag.__init__ (*self*, *asn* = None, *v4* = None, *v6* = None, *valid_until* = None)

Definition at line 465 of file resource_set.py.

7.85.2.3 def rpki.resource_set.resource_bag.__ne__ (*self*, *other*)

Definition at line 514 of file resource_set.py.

7.85.2.4 def rpki.resource_set.resource_bag.__str__ (*self*)

Definition at line 535 of file resource_set.py.

7.85.2.5 def rpki.resource_set.resource_bag.empty (*self*)

```
Return True iff all resource sets in this bag are empty.
```

Definition at line 504 of file resource_set.py.

7.85.2.6 def rpki.resource_set.resource_bag.from_rfc3779_tuples (*cls*, *exts*)

```
Build a resource_bag from intermediate form generated by RFC 3779 ASN.1 decoder.
```

Definition at line 484 of file resource_set.py.

7.85.2.7 def rpki.resource_set.resource_bag.intersection (*self*, *other*)

```
Compute intersection with another resource_bag.
valid_until attribute (if any) inherits from self.
```

Definition at line 517 of file resource_set.py.

7.85.2.8 def rpki.resource_set.resource_bag.oversized (*self*, *other*)

```
True iff self is oversized with respect to other.
```

Definition at line 471 of file resource_set.py.

7.85.2.9 def rpki.resource_set.resource_bag.undersized (*self*, *other*)

```
True iff self is undersized with respect to other.
```

Definition at line 477 of file resource_set.py.

7.85.2.10 def rpki.resource_set.resource_bag.union (*self*, *other*)

```
Compute union with another resource_bag.
valid_until attribute (if any) inherits from self.
```

Definition at line 526 of file resource_set.py.

7.85.3 Member Data Documentation

7.85.3.1 rpki::resource_set.resource_bag::asn

Set of Autonomous System Number resources.

Definition at line 466 of file resource_set.py.

7.85.3.2 rpki::resource_set.resource_bag::v4

Set of IPv4 resources.

Definition at line 467 of file resource_set.py.

7.85.3.3 rpki::resource_set.resource_bag::v6

Set of IPv6 resources.

Definition at line 468 of file resource_set.py.

7.85.3.4 rpki::resource_set.resource_bag::valid_until

Expiration date of resources, for setting certificate notAfter field.

Definition at line 469 of file resource_set.py.

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

- resource_set.py (1873)

7.86 rpki.resource_set.resource_range Class Reference

Inheritance diagram for rpki.resource_set.resource_range:

Public Member Functions

- def __cmp__
- def __init__

Public Attributes

- max
- min

7.86.1 Detailed Description

```
Generic resource range type.  Assumes underlying type is some
kind of integer.

This is a virtual class.  You probably don't want to use this type
directly.
```

Definition at line 35 of file resource_set.py.

7.86.2 Member Function Documentation

7.86.2.1 def rpki.resource_set.resource_range.__cmp__ (*self*, *other*)

```
Compare two resource_range objects.
```

Definition at line 49 of file resource_set.py.

7.86.2.2 def rpki.resource_set.resource_range.__init__ (*self*, *min*, *max*)

```
Initialize and sanity check a resource_range.
```

Definition at line 43 of file resource_set.py.

7.86.3 Member Data Documentation

7.86.3.1 rpki.resource_set.resource_range.max

Definition at line 47 of file resource_set.py.

7.86.3.2 rpki.resource_set.resource_range.min

Reimplemented in rpki.resource_set.resource_range_as.

Definition at line 46 of file resource_set.py.

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

- resource_set.py (1873)

7.87 rpki.resource_set.resource_range_as Class Reference

Inheritance diagram for rpki.resource_set.resource_range_as:

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).

7.87.1 Detailed Description

```
Range of Autonomous System Numbers.

Denotes a single ASN by a range whose min and max values are identical.
```

Definition at line 58 of file resource_set.py.

7.87.2 Member Function Documentation

7.87.2.1 def rpki.resource_set.resource_range_as.__str__ (*self*)

```
Convert a resource_range_as to string format.
```

Definition at line 69 of file resource_set.py.

7.87.2.2 def rpki.resource_set.resource_range_as.to_rfc3779_tuple (*self*)

```
Convert a resource_range_as to tuple format for RFC 3779 ASN.1 encoding.
```

Definition at line 76 of file resource_set.py.

7.87.3 Member Data Documentation

7.87.3.1 rpki::resource_set.resource_range_as::datum_type = long [static]

Type of underlying data (min and max).

Definition at line 67 of file resource_set.py.

7.87.3.2 rpki.resource_set.resource_range_as.min

Reimplemented from rpki.resource_set.resource_range.

Definition at line 71 of file resource_set.py.

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

- resource_set.py (1873)

7.88 rpki.resource_set.resource_range_ip Class Reference

Inheritance diagram for rpki.resource_set.resource_range_ip:

Public Member Functions

- def __str__
- def make_prefix
- def to_rfc3779_tuple

Private Member Functions

- def _prefixlen

7.88.1 Detailed Description

```
Range of (generic) IP addresses.

Prefixes are converted to ranges on input, and ranges that can be
represented as prefixes are written as prefixes on output.

This is a virtual class.  You probably don't want to use it directly.
```

Definition at line 83 of file resource_set.py.

7.88.2 Member Function Documentation

7.88.2.1 def rpki.resource_set.resource_range_ip.__str__ (*self*)

```
Convert a resource_range_ip to string format.
```

Definition at line 106 of file resource_set.py.

7.88.2.2 def rpki.resource_set.resource_range_ip._prefixlen (*self*) [private]

```
Determine whether a resource_range_ip can be expressed as a prefix.
```

Definition at line 92 of file resource_set.py.

7.88.2.3 def rpki.resource_set.resource_range_ip.make_prefix (*cls*, *address*, *prefixlen*)

```
Construct a resource range corresponding to a prefix.
```

Definition at line 124 of file resource_set.py.

7.88.2.4 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 114 of file resource_set.py.

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

- resource_set.py (1873)

7.89 rpki.resource_set.resource_range_ipv4 Class Reference

Inheritance diagram for rpki.resource_set.resource_range_ipv4:

Static Public Attributes

- datum_type = rpki.ipaddrs.v4addr

  Type of underlying data (min and max).

7.89.1 Detailed Description

```
Range of IPv4 addresses.
```

Definition at line 132 of file resource_set.py.

7.89.2 Member Data Documentation

7.89.2.1 rpki::resource_set.resource_range_ipv4::datum_type = rpki.ipaddrs.v4addr [static]

Type of underlying data (min and max).

Definition at line 138 of file resource_set.py.

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

- resource_set.py (1873)

7.90 rpki.resource_set.resource_range_ipv6 Class Reference

Inheritance diagram for rpki.resource_set.resource_range_ipv6:

Static Public Attributes

- datum_type = rpki.ipaddrs.v6addr

  Type of underlying data (min and max).

7.90.1 Detailed Description

```
Range of IPv6 addresses.
```

Definition at line 140 of file resource_set.py.

7.90.2 Member Data Documentation

7.90.2.1 rpki::resource_set.resource_range_ipv6::datum_type = rpki.ipaddrs.v6addr [static]

Type of underlying data (min and max).

Definition at line 146 of file resource_set.py.

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

- resource_set.py (1873)

7.91 rpki.resource_set.resource_set Class Reference

Inheritance diagram for rpki.resource_set.resource_set:

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

7.91.1 Detailed Description

```
Generic resource set.
This is a list subclass containing resource ranges.

This is a virtual class.  You probably don't want to use it
directly.
```

Definition at line 162 of file resource_set.py.

7.91.2 Member Function Documentation

7.91.2.1 def rpki.resource_set.resource_set.__init__ (*self*, *ini* = `None`)

```
Initialize a resource_set.
```

Definition at line 175 of file resource_set.py.

7.91.2.2 def rpki.resource_set.resource_set.__str__ (*self*)

```
Convert a resource_set to string format.
```

Definition at line 199 of file resource_set.py.

7.91.2.3 def rpki.resource_set.resource_set._comm (*self*, *other*) [private]

```
Like comm(1), sort of.

Returns a tuple of three resource sets: resources only in self,
resources only in other, and resources in both.  Used (not very
efficiently) as the basis for most set operations on resource
sets.
```

Definition at line 206 of file resource_set.py.

7.91.2.4 def rpki.resource_set.resource_set.contains (*self*, *item*)

```
Set membership test for resource sets.
```

Definition at line 274 of file resource_set.py.

7.91.2.5 def rpki.resource_set.resource_set.difference (*self*, *other*)

```
Set difference for resource sets.
```

Definition at line 265 of file resource_set.py.

7.91.2.6 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 298 of file resource_set.py.

7.91.2.7 def rpki.resource_set.resource_set.intersection (*self*, *other*)

```
Set intersection for resource sets.
```

Definition at line 261 of file resource_set.py.

7.91.2.8 def rpki.resource_set.resource_set.issubset (*self*, *other*)

```
Test whether self is a subset (possibly improper) of other.
```

Definition at line 286 of file resource_set.py.

7.91.2.9 def rpki.resource_set.resource_set.issuperset (*self*, *other*)

```
Test whether self is a superset (possibly improper) of other.
```

Definition at line 293 of file resource_set.py.

7.91.2.10 def rpki.resource_set.resource_set.symmetric_difference (*self*, *other*)

```
Set symmetric difference (XOR) for resource sets.
```

Definition at line 269 of file resource_set.py.

7.91.2.11 def rpki.resource_set.resource_set.union (*self*, *other*)

```
Set union for resource sets.
```

Definition at line 238 of file resource_set.py.

7.91.3 Member Data Documentation

7.91.3.1 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 173 of file resource_set.py.

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

- resource_set.py (1873)

7.92 rpki.resource_set.resource_set_as Class Reference

Inheritance diagram for rpki.resource_set.resource_set_as:

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.

7.92.1 Detailed Description

```
ASN resource set.
```

Definition at line 312 of file resource_set.py.

7.92.2 Member Function Documentation

7.92.2.1 def rpki.resource_set.resource_set_as.parse_rfc3779_tuple (*self*, *x*)

```
Parse ASN resource from tuple format generated by RFC 3779 ASN.1 decoder.
```

Definition at line 328 of file resource_set.py.

7.92.2.2 def rpki.resource_set.resource_set_as.parse_str (*self*, *x*)

```
Parse ASN resource sets from text (eg, XML attributes).
```

Definition at line 320 of file resource_set.py.

7.92.2.3 def rpki.resource_set.resource_set_as.to_rfc3779_tuple (*self*)

```
Convert ASN resource set into tuple format used for RFC 3779 ASN.1 encoding.
```

Definition at line 343 of file resource_set.py.

7.92.3 Member Data Documentation

7.92.3.1 rpki.resource_set.resource_set_as.inherit

Boolean indicating whether this resource_set uses RFC 3779 inheritance.

Reimplemented from rpki.resource_set.resource_set.

Definition at line 341 of file resource_set.py.

7.92.3.2 rpki::resource_set.resource_set_as::range_type = resource_range_as [static]

Type of range underlying this type of resource_set.

Definition at line 318 of file resource_set.py.

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

- resource_set.py (1873)

7.93 rpki.resource_set.resource_set_ip Class Reference

Inheritance diagram for rpki.resource_set.resource_set_ip:

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.

7.93.1 Detailed Description

```
(Generic) IP address resource set.

This is a virtual class.  You probably don't want to use it
directly.
```

Definition at line 352 of file resource_set.py.

7.93.2 Member Function Documentation

7.93.2.1 def rpki.resource_set.resource_set_ip.parse_rfc3779_tuple (*self*, *x*)

```
Parse IP address resource sets from tuple format generated by RFC 3779 ASN.1 decoder.
```

Definition at line 369 of file resource_set.py.

7.93.2.2 def rpki.resource_set.resource_set_ip.parse_str (*self*, *x*)

```
Parse IP address resource sets from text (eg, XML attributes).
```

Definition at line 359 of file resource_set.py.

7.93.2.3 def rpki.resource_set.resource_set_ip.to_rfc3779_tuple (*self*)

```
Convert IP resource set into tuple format used by RFC 3779 ASN.1 encoder.
```

Definition at line 387 of file resource_set.py.

7.93.3 Member Data Documentation

7.93.3.1 rpki.resource_set.resource_set_ip.inherit

Boolean indicating whether this resource_set uses RFC 3779 inheritance.

Reimplemented from rpki.resource_set.resource_set.

Definition at line 385 of file resource_set.py.

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

- resource_set.py (1873)

7.94 rpki.resource_set.resource_set_ipv4 Class Reference

Inheritance diagram for rpki.resource_set.resource_set_ipv4:

Static Public Attributes

- string afi = "\x00\x01"

  Address Family Identifier value for IPv4.

- range_type = resource_range_ipv4

Type of range underlying this type of resource_set.

7.94.1 Detailed Description

`IPv4 address resource set.`

Definition at line 396 of file resource_set.py.

7.94.2 Member Data Documentation

7.94.2.1 rpki::resource_set.resource_set_ipv4::afi = "\x00\x01" [static]

Address Family Identifier value for IPv4.

Definition at line 407 of file resource_set.py.

7.94.2.2 rpki::resource_set.resource_set_ipv4::range_type = resource_range_ipv4 [static]

Type of range underlying this type of resource_set.

Definition at line 402 of file resource_set.py.

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

- resource_set.py (1873)

7.95 rpki.resource_set.resource_set_ipv6 Class Reference

Inheritance diagram for rpki.resource_set.resource_set_ipv6:

Static Public Attributes

- string afi = "\x00\x02"

  Address Family Identifier value for IPv6.

- range_type = resource_range_ipv6

Type of range underlying this type of resource_set.

7.95.1 Detailed Description

`IPv6 address resource set.`

Definition at line 409 of file resource_set.py.

7.95.2 Member Data Documentation

7.95.2.1 rpki::resource_set.resource_set_ipv6::afi = "\x00\x02" [static]

Address Family Identifier value for IPv6.

Definition at line 420 of file resource_set.py.

7.95.2.2 rpki::resource_set.resource_set_ipv6::range_type = resource_range_ipv6 [static]

Type of range underlying this type of resource_set.

Definition at line 415 of file resource_set.py.

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

- resource_set.py (1873)

7.96 rpki.resource_set.roa_prefix Class Reference

Inheritance diagram for rpki.resource_set.roa_prefix:

Public Member Functions

- def __cmp__
- def __init__
- def __str__
- def max
- def min
- def to_resource_range
- def to_roa_tuple

Public Attributes

- address

  Address portion of prefix.

- max_prefixlen

  Maxmimum prefix length.

- prefixlen

  (Minimum) prefix length.

7.96.1 Detailed Description

```
ROA prefix.  This is similar to the resource_range_ip class, but
differs in that it only represents prefixes, never ranges, and
includes the maximum prefix length as an additional value.

This is a virtual class, you probably don't want to use it directly.
```

Definition at line 557 of file resource_set.py.

7.96.2 Member Function Documentation

7.96.2.1 def rpki.resource_set.roa_prefix.__cmp__ (*self*, *other*)

```
Compare two ROA prefix objects.  Comparision is based on
address, prefixlen, and max_prefixlen, in that order.
```

Definition at line 586 of file resource_set.py.

7.96.2.2 def rpki.resource_set.roa_prefix.__init__ (*self*, *address*, *prefixlen*, *max_prefixlen* = `None`)

```
Initialize a ROA prefix.  max_prefixlen is optional and
defaults to prefixlen.  max_prefixlen must not be smaller than
prefixlen.
```

Definition at line 574 of file resource_set.py.

7.96.2.3 def rpki.resource_set.roa_prefix.__str__ (*self*)

```
Convert a ROA prefix to string format.
```

Definition at line 598 of file resource_set.py.

7.96.2.4 def rpki.resource_set.roa_prefix.max (*self*)

```
Return highest address covered by prefix.
```

Definition at line 616 of file resource_set.py.

7.96.2.5 def rpki.resource_set.roa_prefix.min (*self*)

```
Return lowest address covered by prefix.
```

Definition at line 612 of file resource_set.py.

7.96.2.6 def rpki.resource_set.roa_prefix.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.
```

Definition at line 605 of file resource_set.py.

7.96.2.7 def rpki.resource_set.roa_prefix.to_roa_tuple (*self*)

```
Convert a resource_range_ip to tuple format for ROA ASN.1 encoding.
```

Definition at line 621 of file resource_set.py.

7.96.3 Member Data Documentation

7.96.3.1 rpki::resource_set.roa_prefix::address

Address portion of prefix.

Definition at line 582 of file resource_set.py.

7.96.3.2 rpki::resource_set.roa_prefix::max_prefixlen

Maxmimum prefix length.

Definition at line 584 of file resource_set.py.

7.96.3.3 rpki::resource_set.roa_prefix::prefixlen

(Minimum) prefix length.

Definition at line 583 of file resource_set.py.

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

- resource_set.py (1873)

7.97 rpki.resource_set.roa_prefix_ipv4 Class Reference

Inheritance diagram for rpki.resource_set.roa_prefix_ipv4:

Static Public Attributes

- range_type = resource_range_ipv4

  Type of corresponding resource_range_ip.

7.97.1 Detailed Description

```
IPv4 ROA prefix.
```

Definition at line 626 of file resource_set.py.

7.97.2 Member Data Documentation

7.97.2.1 rpki::resource_set.roa_prefix_ipv4::range_type = resource_range_ipv4 [static]

Type of corresponding resource_range_ip.

Definition at line 632 of file resource_set.py.

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

- resource_set.py (1873)

7.98 rpki.resource_set.roa_prefix_ipv6 Class Reference

Inheritance diagram for rpki.resource_set.roa_prefix_ipv6:

Static Public Attributes

- range_type = resource_range_ipv6

  Type of corresponding resource_range_ip.

7.98.1 Detailed Description

```
IPv6 ROA prefix.
```

Definition at line 634 of file resource_set.py.

7.98.2 Member Data Documentation

7.98.2.1 rpki::resource_set.roa_prefix_ipv6::range_type = resource_range_ipv6 [static]

Type of corresponding resource_range_ip.

Definition at line 640 of file resource_set.py.

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

- resource_set.py (1873)

7.99 rpki.resource_set.roa_prefix_set Class Reference

Inheritance diagram for rpki.resource_set.roa_prefix_set:

Public Member Functions

- def __init__
- def __str__
- def from_sql
- def parse_str
- def to_resource_set
- def to_roa_tuple

7.99.1 Detailed Description

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

Definition at line 642 of file resource_set.py.

7.99.2 Member Function Documentation

7.99.2.1 def rpki.resource_set.roa_prefix_set.__init__ (*self*, *ini* = None)

```
Initialize a ROA prefix set.
```

Definition at line 645 of file resource_set.py.

7.99.2.2 def rpki.resource_set.roa_prefix_set.__str__ (*self*)

```
Convert a ROA prefix set to string format.
```

Definition at line 658 of file resource_set.py.

7.99.2.3 def rpki.resource_set.roa_prefix_set.from_sql (*cls*, *sql*, *query*, *args* = None)

```
Create ROA prefix set from an SQL query.

sql is an object that supports execute() and fetchall() methods
like a DB API 2.0 cursor object.

query is an SQL query that returns a sequence of (address,
prefixlen, max_prefixlen) triples.
```

Definition at line 679 of file resource_set.py.

7.99.2.4 def rpki.resource_set.roa_prefix_set.parse_str (*self*, *x*)

```
Parse ROA prefix from text (eg, an XML attribute).
```

Definition at line 662 of file resource_set.py.

7.99.2.5 def rpki.resource_set.roa_prefix_set.to_resource_set (*self*)

```
Convert a ROA prefix set to a resource set.  This is an
irreversable transformation.
```

Definition at line 672 of file resource_set.py.

7.99.2.6 def rpki.resource_set.roa_prefix_set.to_roa_tuple (*self*)

```
Convert ROA prefix set into tuple format used by ROA ASN.1 encoder.
   This is a variation on the format used in RFC 3779.
```

Definition at line 693 of file resource_set.py.

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

- resource_set.py (1873)

7.100 rpki.resource_set.roa_prefix_set_ipv4 Class Reference

Inheritance diagram for rpki.resource_set.roa_prefix_set_ipv4:

Static Public Attributes

- prefix_type = roa_prefix_ipv4

  Type of underlying roa_prefix.

- resource_set_type = resource_set_ipv4

  Type of corresponding resource_set_ip class.

7.100.1 Detailed Description

```
Set of IPv4 ROA prefixes.
```

Definition at line 701 of file resource_set.py.

7.100.2 Member Data Documentation

7.100.2.1 rpki::resource_set.roa_prefix_set_ipv4::prefix_type = roa_prefix_ipv4 [static]

Type of underlying roa_prefix.

Definition at line 707 of file resource_set.py.

7.100.2.2 rpki::resource_set.roa_prefix_set_ipv4::resource_set_type = resource_set_ipv4 [static]

Type of corresponding resource_set_ip class.

Definition at line 712 of file resource_set.py.

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

- resource_set.py (1873)

7.101 rpki.resource_set.roa_prefix_set_ipv6 Class Reference

Inheritance diagram for rpki.resource_set.roa_prefix_set_ipv6:

Static Public Attributes

- prefix_type = roa_prefix_ipv6

  Type of underlying roa_prefix.

- resource_set_type = resource_set_ipv6

  Type of corresponding resource_set_ip class.

7.101.1 Detailed Description

```
Set of IPv6 ROA prefixes.
```

Definition at line 714 of file resource_set.py.

7.101.2 Member Data Documentation

7.101.2.1 rpki::resource_set.roa_prefix_set_ipv6::prefix_type = roa_prefix_ipv6 [static]

Type of underlying roa_prefix.

Definition at line 720 of file resource_set.py.

7.101.2.2 rpki::resource_set.roa_prefix_set_ipv6::resource_set_type = resource_set_ipv6 [static]

Type of corresponding resource_set_ip class.

Definition at line 725 of file resource_set.py.

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

- resource_set.py (1873)

7.102 rpki.roa.ROAIPAddress Class Reference

Inheritance diagram for rpki.roa.ROAIPAddress:

Public Member Functions

- def __init__

Public Attributes

- address
- maxLength

7.102.1 Detailed Description

Definition at line 65 of file roa.py.

7.102.2 Member Function Documentation

7.102.2.1 def rpki.roa.ROAIPAddress.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 66 of file roa.py.

7.102.3 Member Data Documentation

7.102.3.1 rpki.roa.ROAIPAddress.address

Definition at line 67 of file roa.py.

7.102.3.2 rpki.roa.ROAIPAddress.maxLength

Definition at line 68 of file roa.py.

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

- roa.py (1873)

7.103 rpki.roa.ROAIPAddresses Class Reference

Inheritance diagram for rpki.roa.ROAIPAddresses:

Public Member Functions

- def __init__

7.103.1 Detailed Description

Definition at line 72 of file roa.py.

7.103.2 Member Function Documentation

7.103.2.1 def rpki.roa.ROAIPAddresses.__init__ (*self*, *optional* = 0, *default* = "")

Definition at line 73 of file roa.py.

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

- roa.py (1873)

7.104 rpki.roa.ROAIPAddressFamilies Class Reference

Inheritance diagram for rpki.roa.ROAIPAddressFamilies:

Public Member Functions

- def __init__

7.104.1 Detailed Description

Definition at line 83 of file roa.py.

7.104.2 Member Function Documentation

7.104.2.1 def rpki.roa.ROAIPAddressFamilies.__init__ (*self*, *optional* = 0, *default* = '')

Definition at line 84 of file roa.py.

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

- roa.py (1873)

7.105 rpki.roa.ROAIPAddressFamily Class Reference

Inheritance diagram for rpki.roa.ROAIPAddressFamily:

Public Member Functions

- def __init__

Public Attributes

- addresses
- addressFamily

7.105.1 Detailed Description

Definition at line 76 of file roa.py.

7.105.2 Member Function Documentation

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

Definition at line 77 of file roa.py.

7.105.3 Member Data Documentation

7.105.3.1 rpki.roa.ROAIPAddressFamily.addresses

Definition at line 79 of file roa.py.

7.105.3.2 rpki.roa.ROAIPAddressFamily.addressFamily

Definition at line 78 of file roa.py.

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

- roa.py (1873)

7.106 rpki.roa.RouteOriginAttestation Class Reference

Inheritance diagram for rpki.roa.RouteOriginAttestation:

Public Member Functions

- def __init__

Public Attributes

- asID
- explicitVersion
- ipAddrBlocks
- version

7.106.1 Detailed Description

Definition at line 87 of file roa.py.

7.106.2 Member Function Documentation

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

Definition at line 88 of file roa.py.

7.106.3 Member Data Documentation

7.106.3.1 rpki.roa.RouteOriginAttestation.asID

Definition at line 91 of file roa.py.

7.106.3.2 rpki.roa.RouteOriginAttestation.explicitVersion

Definition at line 90 of file roa.py.

7.106.3.3 rpki.roa.RouteOriginAttestation.ipAddrBlocks

Definition at line 92 of file roa.py.

7.106.3.4 rpki.roa.RouteOriginAttestation.version

Definition at line 89 of file roa.py.

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

- roa.py (1873)

7.107 rpki.rpki_engine.ca_detail_obj Class Reference

Inheritance diagram for rpki.rpki_engine.ca_detail_obj:

Public Member Functions

- def activate
- def ca
- def child_certs
- def create

- def crl_uri
- def delete
- def generate_crl
- def generate_manifest
- def generate_manifest_cert
- def issue
- def issue_ee
- def manifest_uri
- def revoke
- def revoked_certs
- def route_origins
- def sql_decode
- def update

Public Attributes

- ca_cert_uri
- ca_id
- gctx
- latest_ca_cert
- latest_crl
- latest_manifest
- latest_manifest_cert
- manifest_private_key_id
- manifest_public_key
- private_key_id
- public_key
- state

Static Public Attributes

- tuple sql_template

7.107.1 Detailed Description

```
Internal CA detail object.
```

Definition at line 332 of file rpki_engine.py.

7.107.2 Member Function Documentation

7.107.2.1 def rpki.rpki_engine.ca_detail_obj.activate (*self*, *ca*, *cert*, *uri*, *predecessor* = None)

```
Activate this ca_detail.
```

Definition at line 382 of file rpki_engine.py.

7.107.2.2 def rpki.rpki_engine.ca_detail_obj.ca (*self*)

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

Definition at line 358 of file rpki_engine.py.

7.107.2.3 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 362 of file rpki_engine.py.

7.107.2.4 def rpki.rpki_engine.ca_detail_obj.create (*cls*, *ca*)

```
Create a new ca_detail object for a specified CA.
```

Definition at line 487 of file rpki_engine.py.

7.107.2.5 def rpki.rpki_engine.ca_detail_obj.crl_uri (*self*, *ca*)

```
Return publication URI for this ca_detail's CRL.
```

Definition at line 374 of file rpki_engine.py.

7.107.2.6 def rpki.rpki_engine.ca_detail_obj.delete (*self*, *ca*, *repository*)

```
Delete this ca_detail and all of the certs it issued.
```

Definition at line 401 of file rpki_engine.py.

7.107.2.7 def rpki.rpki_engine.ca_detail_obj.generate_crl (*self*, *nextUpdate* = None)

```
Generate a new CRL for this ca_detail.  At the moment this is
unconditional, that is, it is up to the caller to decide whether a
new CRL is needed.
```

Definition at line 571 of file rpki_engine.py.

7.107.2.8 def rpki.rpki_engine.ca_detail_obj.generate_manifest (*self*, *nextUpdate* = None)

```
Generate a new manifest for this ca_detail.
```

Definition at line 604 of file rpki_engine.py.

7.107.2.9 def rpki.rpki_engine.ca_detail_obj.generate_manifest_cert (*self*, *ca*)

```
Generate a new manifest certificate for this ca_detail.
```

Definition at line 520 of file rpki_engine.py.

7.107.2.10 def rpki.rpki_engine.ca_detail_obj.issue (*self*, *ca*, *child*, *subject_key*, *sia*, *resources*, *child_cert* = None)

```
Issue a new certificate to a child.  Optional child_cert
argument specifies an existing child_cert object to update in
place; if not specified, we create a new one.  Returns the
child_cert object containing the newly issued cert.
```

Definition at line 530 of file rpki_engine.py.

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

```
Issue a new EE certificate.
```

Definition at line 505 of file rpki_engine.py.

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

```
Return publication URI for this ca_detail's manifest.
```

Definition at line 378 of file rpki_engine.py.

7.107.2.13 def rpki.rpki_engine.ca_detail_obj.revoke (*self*)

```
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.

- Destroy old keypair (and manifest keypair).

- Leave final CRL in place until its next CRL time has passed.
```

Definition at line 415 of file rpki_engine.py.

7.107.2.14 def rpki.rpki_engine.ca_detail_obj.revoked_certs (*self*)

```
Fetch all revoked_cert objects that link to this ca_detail.
```

Definition at line 366 of file rpki_engine.py.

7.107.2.15 def rpki.rpki_engine.ca_detail_obj.route_origins (*self*)

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

Definition at line 370 of file rpki_engine.py.

7.107.2.16 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_persistant.

Definition at line 350 of file rpki_engine.py.

7.107.2.17 def rpki.rpki_engine.ca_detail_obj.update (*self*, *parent*, *ca*, *rc*, *sia_uri_changed*, *old_resources*)

```
Need to get a new certificate for this ca_detail and perhaps
frob children of this ca_detail.
```

Definition at line 467 of file rpki_engine.py.

7.107.3 Member Data Documentation

7.107.3.1 rpki.rpki_engine.ca_detail_obj.ca_cert_uri

Definition at line 386 of file rpki_engine.py.

7.107.3.2 rpki.rpki_engine.ca_detail_obj.ca_id

Definition at line 491 of file rpki_engine.py.

7.107.3.3 rpki.rpki_engine.ca_detail_obj.gctx

Reimplemented from rpki.sql.sql_persistant.

Definition at line 490 of file rpki_engine.py.

7.107.3.4 rpki.rpki_engine.ca_detail_obj.latest_ca_cert

Definition at line 385 of file rpki_engine.py.

7.107.3.5 rpki.rpki_engine.ca_detail_obj.latest_crl

Definition at line 594 of file rpki_engine.py.

7.107.3.6 rpki.rpki_engine.ca_detail_obj.latest_manifest

Definition at line 619 of file rpki_engine.py.

7.107.3.7 rpki.rpki_engine.ca_detail_obj.latest_manifest_cert

Definition at line 463 of file rpki_engine.py.

7.107.3.8 rpki.rpki_engine.ca_detail_obj.manifest_private_key_id

Definition at line 461 of file rpki_engine.py.

7.107.3.9 rpki.rpki_engine.ca_detail_obj.manifest_public_key

Definition at line 462 of file rpki_engine.py.

7.107.3.10 rpki.rpki_engine.ca_detail_obj.private_key_id

Definition at line 460 of file rpki_engine.py.

7.107.3.11 rpki.rpki_engine.ca_detail_obj.public_key

Definition at line 496 of file rpki_engine.py.

7.107.3.12 tuple rpki.rpki_engine.ca_detail_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
    "ca_detail",
    "ca_detail_id",
    ("private_key_id",          rpki.x509.RSA),
    ("public_key",              rpki.x509.RSApublic),
    ("latest_ca_cert",          rpki.x509.X509),
    ("manifest_private_key_id", rpki.x509.RSA),
    ("manifest_public_key",     rpki.x509.RSApublic),
    ("latest_manifest_cert",    rpki.x509.X509),
    ("latest_manifest",         rpki.x509.SignedManifest),
    ("latest_crl",              rpki.x509.CRL),
    "state",
    "ca_cert_uri",
    "ca_id")
```

Definition at line 335 of file rpki_engine.py.

7.107.3.13 rpki.rpki_engine.ca_detail_obj.state

Definition at line 390 of file rpki_engine.py.

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

- rpki_engine.py (1873)

7.108 rpki.rpki_engine.ca_obj Class Reference

Inheritance diagram for rpki.rpki_engine.ca_obj:

Public Member Functions

- def ca_details
- def check_for_updates
- def construct_sia_uri
- def create

- def delete
- def fetch_active
- def fetch_deprecated
- def fetch_pending
- def fetch_revoked
- def next_crl_number
- def next_manifest_number
- def next_serial_number
- def parent
- def rekey
- def revoke

Public Attributes

- gctx
- parent_id
- parent_resource_class
- sia_uri

Static Public Attributes

- int last_crl_sn = 0
- int last_issued_sn = 0
- int last_manifest_sn = 0
- tuple sql_template

7.108.1 Detailed Description

```
Internal CA object.
```

Definition at line 160 of file rpki_engine.py.

7.108.2 Member Function Documentation

7.108.2.1 def rpki.rpki_engine.ca_obj.ca_details (*self*)

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

Definition at line 180 of file rpki_engine.py.

7.108.2.2 def rpki.rpki_engine.ca_obj.check_for_updates (*self*, *parent*, *rc*)

```
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 213 of file rpki_engine.py.

7.108.2.3 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 200 of file rpki_engine.py.

7.108.2.4 def rpki.rpki_engine.ca_obj.create (*cls*, *parent*, *rc*)

```
Parent has signaled existance of a new resource class, so we
need to create and set up a corresponding CA object.
```

Definition at line 247 of file rpki_engine.py.

7.108.2.5 def rpki.rpki_engine.ca_obj.delete (*self*, *parent*)

```
The list of current resource classes received from parent does
not include the class corresponding to this CA, so we need to
delete it (and its little dog too...).

All certs published by this CA are now invalid, so need to
withdraw them, the CRL, and the manifest from the repository,
delete all child_cert and ca_detail records associated with this
CA, then finally delete this CA itself.
```

Definition at line 268 of file rpki_engine.py.

7.108.2.6 def rpki.rpki_engine.ca_obj.fetch_active (*self*)

```
Fetch the active ca_detail for this CA, if any.
```

Definition at line 188 of file rpki_engine.py.

7.108.2.7 def rpki.rpki_engine.ca_obj.fetch_deprecated (*self*)

```
Fetch deprecated ca_details for this CA, if any.
```

Definition at line 192 of file rpki_engine.py.

7.108.2.8 def rpki.rpki_engine.ca_obj.fetch_pending (*self*)

```
Fetch the pending ca_details for this CA, if any.
```

Definition at line 184 of file rpki_engine.py.

7.108.2.9 def rpki.rpki_engine.ca_obj.fetch_revoked (*self*)

```
Fetch revoked ca_details for this CA, if any.
```

Definition at line 196 of file rpki_engine.py.

7.108.2.10 def rpki.rpki_engine.ca_obj.next_crl_number (*self*)

```
Allocate a CRL serial number.
```

Definition at line 296 of file rpki_engine.py.

7.108.2.11 def rpki.rpki_engine.ca_obj.next_manifest_number (*self*)

```
Allocate a manifest serial number.
```

Definition at line 290 of file rpki_engine.py.

7.108.2.12 def rpki.rpki_engine.ca_obj.next_serial_number (*self*)

```
Allocate a certificate serial number.
```

Definition at line 284 of file rpki_engine.py.

7.108.2.13 def rpki.rpki_engine.ca_obj.parent (*self*)

```
Fetch parent object to which this CA object links.
```

Definition at line 176 of file rpki_engine.py.

7.108.2.14 def rpki.rpki_engine.ca_obj.rekey (*self*)

```
Initiate a rekey operation for this ca.  Generate a new
keypair.  Request cert from parent using new keypair.  Mark result
as our active ca_detail.  Reissue all child certs issued by this
ca using the new ca_detail.
```

Definition at line 302 of file rpki_engine.py.

7.108.2.15 def rpki.rpki_engine.ca_obj.revoke (*self*)

```
Revoke deprecated ca_detail objects associated with this ca.
```

Definition at line 324 of file rpki_engine.py.

7.108.3 Member Data Documentation

7.108.3.1 rpki.rpki_engine.ca_obj.gctx

Reimplemented from rpki.sql.sql_persistant.

Definition at line 253 of file rpki_engine.py.

7.108.3.2 int rpki.rpki_engine.ca_obj.last_crl_sn = 0 [static]

Definition at line 172 of file rpki_engine.py.

7.108.3.3 int rpki.rpki_engine.ca_obj.last_issued_sn = 0 [static]

Definition at line 173 of file rpki_engine.py.

7.108.3.4 int rpki.rpki_engine.ca_obj.last_manifest_sn = 0 [static]

Definition at line 174 of file rpki_engine.py.

7.108.3.5 rpki.rpki_engine.ca_obj.parent_id

Definition at line 254 of file rpki_engine.py.

7.108.3.6 rpki.rpki_engine.ca_obj.parent_resource_class

Definition at line 255 of file rpki_engine.py.

7.108.3.7 rpki.rpki_engine.ca_obj.sia_uri

Definition at line 223 of file rpki_engine.py.

7.108.3.8 tuple rpki.rpki_engine.ca_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
    "ca",
    "ca_id",
    "last_crl_sn",
    ("next_crl_update", rpki.sundial.datetime),
    "last_issued_sn", "last_manifest_sn",
    ("next_manifest_update", rpki.sundial.datetime),
    "sia_uri", "parent_id", "parent_resource_class")
```

Definition at line 163 of file rpki_engine.py.

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

- rpki_engine.py (1873)

7.109 rpki.rpki_engine.child_cert_obj Class Reference

Inheritance diagram for rpki.rpki_engine.child_cert_obj:

Public Member Functions

- def __init__
- def ca_detail
- def child
- def fetch

- def reissue
- def revoke
- def uri
- def uri_tail

Public Attributes

- ca_detail_id
- cert
- child_id
- gctx

Static Public Attributes

- tuple sql_template

7.109.1 Detailed Description

```
Certificate that has been issued to a child.
```

Definition at line 629 of file rpki_engine.py.

7.109.2 Member Function Documentation

7.109.2.1 def rpki.rpki_engine.child_cert_obj.__init__ (*self*, *gctx* = None, *child_id* = None, *ca_detail_id* = None, *cert* = None)

```
Initialize a child_cert_obj.
```

Definition at line 640 of file rpki_engine.py.

7.109.2.2 def rpki.rpki_engine.child_cert_obj.ca_detail (*self*)

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

Definition at line 653 of file rpki_engine.py.

7.109.2.3 def rpki.rpki_engine.child_cert_obj.child (*self*)

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

Definition at line 649 of file rpki_engine.py.

7.109.2.4 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 730 of file rpki_engine.py.

7.109.2.5 def rpki.rpki_engine.child_cert_obj.reissue (*self*, *ca_detail*, *resources* = None, *sia* = None)

```
Reissue an existing cert, reusing the public key.  If the cert
we would generate is identical to the one we already have, we just
return the one we already have.  If we have to revoke the old
certificate when generating the new one, we have to generate a new
child_cert_obj, so calling code that needs the updated
child_cert_obj must use the return value from this method.
```

Definition at line 676 of file rpki_engine.py.

7.109.2.6 def rpki.rpki_engine.child_cert_obj.revoke (*self*)

```
Revoke a child cert.
```

Definition at line 665 of file rpki_engine.py.

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

```
Return the publication URI for this child_cert.
```

Definition at line 661 of file rpki_engine.py.

7.109.2.8 def rpki.rpki_engine.child_cert_obj.uri_tail (*self*)

```
Return the tail (filename) portion of the URI for this child_cert.
```

Definition at line 657 of file rpki_engine.py.

7.109.3 Member Data Documentation

7.109.3.1 rpki.rpki_engine.child_cert_obj.ca_detail_id

Definition at line 644 of file rpki_engine.py.

7.109.3.2 rpki.rpki_engine.child_cert_obj.cert

Definition at line 645 of file rpki_engine.py.

7.109.3.3 rpki.rpki_engine.child_cert_obj.child_id

Definition at line 643 of file rpki_engine.py.

7.109.3.4 rpki.rpki_engine.child_cert_obj.gctx

Reimplemented from rpki.sql.sql_persistant.

Definition at line 642 of file rpki_engine.py.

7.109.3.5 tuple rpki.rpki_engine.child_cert_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
    "child_cert",
    "child_cert_id",
    ("cert", rpki.x509.X509),
    "child_id",
    "ca_detail_id",
    "ski")
```

Definition at line 632 of file rpki_engine.py.

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

- rpki_engine.py (1873)

7.110 rpki.rpki_engine.revoked_cert_obj Class Reference

Inheritance diagram for rpki.rpki_engine.revoked_cert_obj:

Public Member Functions

- def __init__
- def ca_detail
- def revoke

Public Attributes

- ca_detail_id
- expires
- gctx
- revoked
- serial

Static Public Attributes

- tuple sql_template

7.110.1 Detailed Description

```
Tombstone for a revoked certificate.
```

Definition at line 761 of file rpki_engine.py.

7.110.2 Member Function Documentation

7.110.2.1 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 772 of file rpki_engine.py.

7.110.2.2 def rpki.rpki_engine.revoked_cert_obj.ca_detail (*self*)

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

Definition at line 782 of file rpki_engine.py.

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

```
Revoke a certificate.
```

Definition at line 787 of file rpki_engine.py.

7.110.3 Member Data Documentation

7.110.3.1 rpki.rpki_engine.revoked_cert_obj.ca_detail_id

Definition at line 778 of file rpki_engine.py.

7.110.3.2 rpki.rpki_engine.revoked_cert_obj.expires

Definition at line 777 of file rpki_engine.py.

7.110.3.3 rpki.rpki_engine.revoked_cert_obj.gctx

Reimplemented from rpki.sql.sql_persistant.

Definition at line 774 of file rpki_engine.py.

7.110.3.4 rpki.rpki_engine.revoked_cert_obj.revoked

Definition at line 776 of file rpki_engine.py.

7.110.3.5 rpki.rpki_engine.revoked_cert_obj.serial

Definition at line 775 of file rpki_engine.py.

7.110.3.6 tuple rpki.rpki_engine.revoked_cert_obj.sql_template [static]

Initial value:

```
rpki.sql.template(
    "revoked_cert",
    "revoked_cert_id",
    "serial",
    "ca_detail_id",
    ("revoked", rpki.sundial.datetime),
    ("expires", rpki.sundial.datetime))
```

Definition at line 764 of file rpki_engine.py.

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

- rpki_engine.py (1873)

7.111 rpki.rpki_engine.rpkid_context Class Reference

Inheritance diagram for rpki.rpki_engine.rpkid_context:

Public Member Functions

- def __init__
- def build_https_ta_cache
- def clear_https_ta_cache
- def cronjob_handler
- def irdb_query
- def left_right_handler
- def up_down_handler

Public Attributes

- bpki_ta
- https_server_host
- https_server_port
- irbe_cert
- irdb_cert
- irdb_url
- publication_kludge_base

- rpkid_cert
- rpkid_key
- sql

Static Public Attributes

- https_ta_cache = None

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

7.111.1 Detailed Description

```
A container for various global rpkid parameters.
```

Definition at line 24 of file rpki_engine.py.

7.111.2 Member Function Documentation

7.111.2.1 def rpki.rpki_engine.rpkid_context.__init__ (*self*, *cfg*)

Definition at line 27 of file rpki_engine.py.

7.111.2.2 def rpki.rpki_engine.rpkid_context.build_https_ta_cache (*self*)

```
Build dynamic TLS trust anchors.
```

Definition at line 142 of file rpki_engine.py.

7.111.2.3 def rpki.rpki_engine.rpkid_context.clear_https_ta_cache (*self*)

```
Clear dynamic TLS trust anchors.
```

Definition at line 135 of file rpki_engine.py.

7.111.2.4 def rpki.rpki_engine.rpkid_context.cronjob_handler (*self*, *query*, *path*)

```
Periodic tasks.  As simple as possible for now, may need to break
this up into separate handlers later.
```

Definition at line 112 of file rpki_engine.py.

7.111.2.5 def rpki.rpki_engine.rpkid_context.irdb_query (*self*, *self_id*, *child_id* = None)

```
Perform an IRDB callback query.  In the long run this should not
be a blocking routine, it should instead issue a query and set up a
handler to receive the response.  For the moment, though, we are
doing simple lock step and damn the torpedos.  Not yet doing
anything useful with subject name.  Most likely this function should
really be wrapped up in a class that carries both the query result
and also the intermediate state needed for the event-driven code
that this function will need to become.
```

Definition at line 44 of file rpki_engine.py.

7.111.2.6 def rpki.rpki_engine.rpkid_context.left_right_handler (*self*, *query*, *path*)

```
Process one left-right PDU.
```

Definition at line 78 of file rpki_engine.py.

7.111.2.7 def rpki.rpki_engine.rpkid_context.up_down_handler (*self*, *query*, *path*)

```
Process one up-down PDU.
```

Definition at line 94 of file rpki_engine.py.

7.111.3 Member Data Documentation

7.111.3.1 rpki.rpki_engine.rpkid_context.bpki_ta

Definition at line 31 of file rpki_engine.py.

7.111.3.2 rpki.rpki_engine.rpkid_context.https_server_host

Definition at line 39 of file rpki_engine.py.

7.111.3.3 rpki.rpki_engine.rpkid_context.https_server_port

Definition at line 40 of file rpki_engine.py.

7.111.3.4 rpki::rpki_engine.rpkid_context::https_ta_cache = None [static]

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

Definition at line 133 of file rpki_engine.py.

7.111.3.5 rpki.rpki_engine.rpkid_context.irbe_cert

Definition at line 33 of file rpki_engine.py.

7.111.3.6 rpki.rpki_engine.rpkid_context.irdb_cert

Definition at line 32 of file rpki_engine.py.

7.111.3.7 rpki.rpki_engine.rpkid_context.irdb_url

Definition at line 37 of file rpki_engine.py.

7.111.3.8 rpki.rpki_engine.rpkid_context.publication_kludge_base

Definition at line 42 of file rpki_engine.py.

7.111.3.9 rpki.rpki_engine.rpkid_context.rpkid_cert

Definition at line 34 of file rpki_engine.py.

7.111.3.10 rpki.rpki_engine.rpkid_context.rpkid_key

Definition at line 35 of file rpki_engine.py.

7.111.3.11 rpki.rpki_engine.rpkid_context.sql

Definition at line 29 of file rpki_engine.py.

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

- rpki_engine.py (1873)

7.112 rpki.sql.session Class Reference

Inheritance diagram for rpki.sql.session:

Public Member Functions

- def __init__
- def assert_pristine
- def cache_clear
- def close

- def connect
- def execute
- def executemany
- def fetchall
- def lastrowid
- def ping
- def sweep

Public Attributes

- cache
- cur
- database
- db
- dirty
- password
- username

Private Member Functions

- def _wrap_execute

Static Private Attributes

- _exceptions_enabled = False

7.112.1 Detailed Description

```
SQL session layer.
```

Definition at line 23 of file sql.py.

7.112.2 Member Function Documentation

7.112.2.1 def rpki.sql.session.__init__ (*self*, *cfg*)

Definition at line 28 of file sql.py.

7.112.2.2 def rpki.sql.session._wrap_execute (*self*, *func*, *query*, *args*) [private]

Definition at line 58 of file sql.py.

7.112.2.3 def rpki.sql.session.assert_pristine (*self*)

```
Assert that there are no dirty objects in the cache.
```

Definition at line 82 of file sql.py.

7.112.2.4 def rpki.sql.session.cache_clear (*self*)

```
Clear the object cache.
```

Definition at line 78 of file sql.py.

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

Definition at line 47 of file sql.py.

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

Definition at line 43 of file sql.py.

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

Definition at line 66 of file sql.py.

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

Definition at line 69 of file sql.py.

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

Definition at line 72 of file sql.py.

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

Definition at line 75 of file sql.py.

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

Definition at line 55 of file sql.py.

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

```
Write any dirty objects out to SQL.
```

Definition at line 86 of file sql.py.

7.112.3 Member Data Documentation

7.112.3.1 rpki.sql.session._exceptions_enabled = False [static, private]

Definition at line 26 of file sql.py.

7.112.3.2 rpki.sql.session.cache

Definition at line 38 of file sql.py.

7.112.3.3 rpki.sql.session.cur

Definition at line 45 of file sql.py.

7.112.3.4 rpki.sql.session.database

Definition at line 35 of file sql.py.

7.112.3.5 rpki.sql.session.db

Definition at line 44 of file sql.py.

7.112.3.6 rpki.sql.session.dirty

Definition at line 39 of file sql.py.

7.112.3.7 rpki.sql.session.password

Definition at line 36 of file sql.py.

7.112.3.8 rpki.sql.session.username

Definition at line 34 of file sql.py.

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

- sql.py (1873)

7.113 rpki.sql.sql_persistant Class Reference

Inheritance diagram for rpki.sql.sql_persistant:

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.

7.113.1 Detailed Description

```
Mixin for persistant class that needs to be stored in SQL.
```

Definition at line 115 of file sql.py.

7.113.2 Member Function Documentation

7.113.2.1 def rpki.sql.sql_persistant.sql_decode (*self*, *vals*)

```
Initialize an object with values returned by self.sql_fetch().
This is a default version that assumes a one-to-one mapping
between column names in SQL and attribute names in Python.  If you
need something fancier, override this.
```

Reimplemented in rpki.rpki_engine.ca_detail_obj.

Definition at line 262 of file sql.py.

7.113.2.2 def rpki.sql.sql_persistant.sql_delete (*self*)

```
Delete this object from SQL.
```

Definition at line 238 of file sql.py.

7.113.2.3 def rpki.sql.sql_persistant.sql_delete_hook (*self*)

```
Customization hook.
```

Reimplemented in rpki.left_right.route_origin_elt.

Definition at line 287 of file sql.py.

7.113.2.4 def rpki.sql.sql_persistant.sql_encode (*self*)

```
Convert object attributes into a dict for use with canned SQL
queries.  This is a default version that assumes a one-to-one
mapping between column names in SQL and attribute names in Python.
If you need something fancier, override this.
```

Definition at line 250 of file sql.py.

7.113.2.5 def rpki.sql.sql_persistant.sql_fetch (*cls*, *gctx*, *id*)

```
Fetch one object from SQL, based on its primary key.

Since in this one case we know that the primary index is also the
cache key, we check for a cache hit directly in the hope of
bypassing the SQL lookup entirely.

This method is usually called via a one-line class-specific
wrapper.  As a convenience, we also accept an id of None, and just
return None in this case.
```

Definition at line 135 of file sql.py.

7.113.2.6 def rpki.sql.sql_persistant.sql_fetch_all (*cls*, *gctx*)

```
Fetch all objects of this type from SQL.
```

Definition at line 170 of file sql.py.

7.113.2.7 def rpki.sql.sql_persistant.sql_fetch_hook (*self*)

```
Customization hook.
```

Reimplemented in rpki.left_right.route_origin_elt.

Definition at line 274 of file sql.py.

7.113.2.8 def rpki.sql.sql_persistant.sql_fetch_where (*cls*, *gctx*, *where*, *args* = None)

```
Fetch objects of this type matching an arbitrary SQL WHERE expression.
```

Definition at line 175 of file sql.py.

7.113.2.9 def rpki.sql.sql_persistant.sql_fetch_where1 (*cls*, *gctx*, *where*, *args* = None)

```
Fetch one object from SQL, based on an arbitrary SQL WHERE expression.
```

Definition at line 157 of file sql.py.

7.113.2.10 def rpki.sql.sql_persistant.sql_init (*cls*, *gctx*, *row*, *key*)

```
Initialize one Python object from the result of a SQL query.
```

Definition at line 197 of file sql.py.

7.113.2.11 def rpki.sql.sql_persistant.sql_insert_hook (*self*)

```
Customization hook.
```

Reimplemented in rpki.left_right.route_origin_elt.

Definition at line 278 of file sql.py.

7.113.2.12 def rpki.sql.sql_persistant.sql_is_dirty (*self*)

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

Definition at line 215 of file sql.py.

7.113.2.13 def rpki.sql.sql_persistant.sql_mark_clean (*self*)

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

Definition at line 211 of file sql.py.

7.113.2.14 def rpki.sql.sql_persistant.sql_mark_deleted (*self*)

```
Mark this object as needing to be deleted in SQL.
```

Definition at line 219 of file sql.py.

7.113.2.15 def rpki.sql.sql_persistant.sql_mark_dirty (*self*)

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

Definition at line 207 of file sql.py.

7.113.2.16 def rpki.sql.sql_persistant.sql_store (*self*)

```
Store this object to SQL.
```

Definition at line 223 of file sql.py.

7.113.2.17 def rpki.sql.sql_persistant.sql_update_hook (*self*)

```
Customization hook.
```

Definition at line 282 of file sql.py.

7.113.3 Member Data Documentation

7.113.3.1 rpki.sql.sql_persistant.gctx

Reimplemented in rpki.rpki_engine.ca_obj, rpki.rpki_engine.ca_detail_obj, rpki.rpki_engine.child_cert_obj, and rpki.rpki_engine.revoked_cert_obj.

Definition at line 200 of file sql.py.

7.113.3.2 rpki::sql.sql_persistant::sql_debug = False [static]

Enable logging of SQL actions.

Definition at line 132 of file sql.py.

7.113.3.3 rpki::sql.sql_persistant::sql_deleted = False [static]

Whether our cached copy of this object has been deleted.

Definition at line 127 of file sql.py.

7.113.3.4 rpki::sql.sql_persistant::sql_in_db = False [static]

Whether this object is already in SQL or not.

Definition at line 122 of file sql.py.

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

- sql.py (1873)

7.114 rpki.sql.template Class Reference

Inheritance diagram for rpki.sql.template:

Public Member Functions

- def __init__

Public Attributes

- columns
- delete
- index
- insert
- map
- select
- table
- update

7.114.1 Detailed Description

```
SQL template generator.
```

Definition at line 96 of file sql.py.

7.114.2 Member Function Documentation

7.114.2.1 def rpki.sql.template.__init__ (*self*, *table_name*, *index_column*, *data_columns*)

```
Build a SQL template.
```

Definition at line 98 of file sql.py.

7.114.3 Member Data Documentation

7.114.3.1 rpki.sql.template.columns

Definition at line 105 of file sql.py.

7.114.3.2 rpki.sql.template.delete

Definition at line 113 of file sql.py.

7.114.3.3 rpki.sql.template.index

Definition at line 104 of file sql.py.

7.114.3.4 rpki.sql.template.insert

Definition at line 108 of file sql.py.

7.114.3.5 rpki.sql.template.map

Definition at line 106 of file sql.py.

7.114.3.6 rpki.sql.template.select

Definition at line 107 of file sql.py.

7.114.3.7 rpki.sql.template.table

Definition at line 103 of file sql.py.

7.114.3.8 rpki.sql.template.update

Definition at line 110 of file sql.py.

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

- sql.py (1873)

7.115 rpki.sundial.datetime Class Reference

Inheritance diagram for rpki.sundial.datetime:

Public Member Functions

- def __add__
- def __str__
- def __sub__
- def earlier
- def from_sql
- def fromASN1tuple
- def fromdatetime
- def fromGeneralizedTime
- def fromUTCTime
- def fromXMLtime

- def later
- def to_sql
- def toASN1tuple
- def toGeneralizedTime
- def totimestamp
- def toUTCTime
- def toXMLtime

Static Public Attributes

- tuple PKIX_threshhold = pydatetime.datetime(2050, 1, 1)

  Threshold specified in RFC 3280 for switchover from UTCTime to GeneralizedTime.

7.115.1 Detailed Description

```
RPKI extensions to standard datetime.datetime class.  All work
here is in UTC, so we use naive datetime objects.
```

Definition at line 30 of file sundial.py.

7.115.2 Member Function Documentation

7.115.2.1 def rpki.sundial.datetime.__add__ (*self*, *other*)

```
Force correct class for timedelta results.
```

Definition at line 102 of file sundial.py.

7.115.2.2 def rpki.sundial.datetime.__str__ (*self*)

Definition at line 92 of file sundial.py.

7.115.2.3 def rpki.sundial.datetime.__sub__ (*self*, *other*)

```
Force correct class for timedelta results.
```

Definition at line 106 of file sundial.py.

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

```
Return the earlier of two timestamps.
```

Definition at line 133 of file sundial.py.

7.115.2.5 def rpki.sundial.datetime.from_sql (*cls*, *x*)

```
Convert from SQL storage format.
```

Definition at line 111 of file sundial.py.

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

```
Convert from ASN.1 tuple representation.
```

Definition at line 60 of file sundial.py.

7.115.2.7 def rpki.sundial.datetime.fromdatetime (*cls*, *x*)

```
Convert a datetime.datetime object into this subclass.
This is whacky due to the weird constructors for datetime.
```

Definition at line 96 of file sundial.py.

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

```
Convert from ASN.1 GeneralizedTime.
```

Definition at line 51 of file sundial.py.

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

```
Convert from ASN.1 UTCTime.
```

Definition at line 42 of file sundial.py.

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

```
Convert from XML time representation.
```

Definition at line 81 of file sundial.py.

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

```
Return the later of two timestamps.
```

Definition at line 129 of file sundial.py.

7.115.2.12 def rpki.sundial.datetime.to_sql (*self*)

```
Convert to SQL storage format.

There's something whacky going on in the MySQLdb module, it throws
range errors when storing a derived type into a DATETIME column.
Investigate some day, but for now brute force this by copying the
relevant fields into a datetime.datetime for MySQLdb's
consumption.
```

Definition at line 115 of file sundial.py.

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

```
Convert to ASN.1 tuple representation.
```

Definition at line 73 of file sundial.py.

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

```
Convert to ASN.1 GeneralizedTime.
```

Definition at line 55 of file sundial.py.

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

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

Definition at line 35 of file sundial.py.

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

```
Convert to ASN.1 UTCTime.
```

Definition at line 46 of file sundial.py.

7.115.2.17 def rpki.sundial.datetime.toXMLtime (*self*)

```
Convert to XML time representation.
```

Definition at line 88 of file sundial.py.

7.115.3 Member Data Documentation

7.115.3.1 rpki::sundial.datetime::PKIX_threshhold = pydatetime.datetime(2050, 1, 1) [static]

Threshold specified in RFC 3280 for switchover from UTCTime to GeneralizedTime.

Definition at line 71 of file sundial.py.

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

- sundial.py (1873)

7.116 rpki.sundial.timedelta Class Reference

Inheritance diagram for rpki.sundial.timedelta:

Public Member Functions

- def convert_to_seconds
- def parse

Static Public Attributes

- tuple regexp

  Hideously ugly regular expression to parse the complex text form.

7.116.1 Detailed Description

```
Timedelta with text parsing.  This accepts two input formats:

- A simple integer, indicating a number of seconds.

- A string of the form "wD xH yM zS" where w, x, y, and z are integers
  and D, H, M, and S indicate days, hours, minutes, and seconds.
  All of the fields are optional, but at least one must be specified.
  Eg, "3D4H" means "three days plus four hours".
```

Definition at line 137 of file sundial.py.

7.116.2 Member Function Documentation

7.116.2.1 def rpki.sundial.timedelta.convert_to_seconds (*self*)

```
Convert a timedelta interval to seconds.
```

Definition at line 168 of file sundial.py.

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

```
Parse text into a timedelta object.
```

Definition at line 159 of file sundial.py.

7.116.3 Member Data Documentation

7.116.3.1 rpki::sundial.timedelta::regexp [static]

Initial value:

```
re.compile("\\s*(?:(?P<days>\\d+)D)?" +
                      "\\s*(?:(?P<hours>\\d+)H)?" +
                      "\\s*(?:(?P<minutes>\\d+)M)?" +
                      "\\s*(?:(?P<seconds>\\d+)S)?\\s*", re.I)
```

Hideously ugly regular expression to parse the complex text form.

Tags are intended for use with re.MatchObject.groupdict() and map directly to the keywords expected by the timedelta constructor.

Definition at line 153 of file sundial.py.

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

- sundial.py (1873)

7.117 rpki.up_down.base_elt Class Reference

Inheritance diagram for rpki.up_down.base_elt:

Public Member Functions

- def check_response
- def endElement
- def make_b64elt
- def make_elt
- def serve_pdu
- def startElement

7.117.1 Detailed Description

```
Generic PDU object.
```

```
Virtual class, just provides some default methods.
```

Definition at line 28 of file up_down.py.

7.117.2 Member Function Documentation

7.117.2.1 def rpki.up_down.base_elt.check_response (*self*)

```
Placeholder for response checking.
```

Reimplemented in rpki.up_down.issue_response_pdu, and rpki.up_down.error_response_pdu.

Definition at line 69 of file up_down.py.

7.117.2.2 def rpki.up_down.base_elt.endElement (*self*, *stack*, *name*, *text*)

```
Ignore endElement() if there's no specific handler.

If we don't need to do anything else, just pop the stack.
```

Reimplemented in rpki.up_down.certificate_elt, rpki.up_down.class_elt, rpki.up_down.issue_pdu, and rpki.up_down.error_response_pdu.

Definition at line 42 of file up_down.py.

7.117.2.3 def rpki.up_down.base_elt.make_b64elt (*self*, *elt*, *name*, *value* = None)

```
Construct a sub-element with Base64 text content.
```

Definition at line 58 of file up_down.py.

7.117.2.4 def rpki.up_down.base_elt.make_elt (*self*, *name*, *attrs*)

```
Construct a element, copying over a set of attributes.
```

Definition at line 49 of file up_down.py.

7.117.2.5 def rpki.up_down.base_elt.serve_pdu (*self*, *q_msg*, *r_msg*, *child*)

```
Default PDU handler to catch unexpected types.
```

Reimplemented in rpki.up_down.list_pdu, rpki.up_down.issue_pdu, and rpki.up_down.revoke_pdu.

Definition at line 65 of file up_down.py.

7.117.2.6 def rpki.up_down.base_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Ignore startElement() if there's no specific handler.

Some elements have no attributes and we only care about their
text content.
```

Reimplemented in rpki.up_down.certificate_elt, rpki.up_down.class_elt, rpki.up_down.class_response_syntax, rpki.up_down.issue_pdu, rpki.up_down.revoke_syntax, and rpki.up_down.message_pdu.

Definition at line 34 of file up_down.py.

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

- up_down.py (1873)

7.118 rpki.up_down.certificate_elt Class Reference

Inheritance diagram for rpki.up_down.certificate_elt:

Public Member Functions

- def endElement
- def startElement
- def toXML

Public Attributes

- cert
- cert_url
- req_resource_set_as
- req_resource_set_ipv4
- req_resource_set_ipv6

7.118.1 Detailed Description

```
Up-Down protocol representation of an issued certificate.
```

Definition at line 99 of file up_down.py.

7.118.2 Member Function Documentation

7.118.2.1 def rpki.up_down.certificate_elt.endElement (*self*, *stack*, *name*, *text*)

```
Handle text content of a <certificate/> element.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 110 of file up_down.py.

7.118.2.2 def rpki.up_down.certificate_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle attributes of <certificate/> element.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 102 of file up_down.py.

7.118.2.3 def rpki.up_down.certificate_elt.toXML (*self*)

```
Generate a <certificate/> element.
```

Definition at line 116 of file up_down.py.

7.118.3 Member Data Documentation

7.118.3.1 rpki.up_down.certificate_elt.cert

Definition at line 113 of file up_down.py.

7.118.3.2 rpki.up_down.certificate_elt.cert_url

Definition at line 105 of file up_down.py.

7.118.3.3 rpki.up_down.certificate_elt.req_resource_set_as

Definition at line 106 of file up_down.py.

7.118.3.4 rpki.up_down.certificate_elt.req_resource_set_ipv4

Definition at line 107 of file up_down.py.

7.118.3.5 rpki.up_down.certificate_elt.req_resource_set_ipv6

Definition at line 108 of file up_down.py.

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

- up_down.py (1873)

7.119 rpki.up_down.class_elt Class Reference

Inheritance diagram for rpki.up_down.class_elt:

Public Member Functions

- def __init__
- def endElement
- def from_resource_bag
- def startElement

- def to_resource_bag
- def toXML

Public Attributes

- cert_url
- certs
- class_name
- resource_set_as
- resource_set_ipv4
- resource_set_ipv6
- resource_set_notafter
- suggested_sia_head

Static Public Attributes

- issuer = None

7.119.1 Detailed Description

```
Up-Down protocol representation of a resource class.
```

Definition at line 123 of file up_down.py.

7.119.2 Member Function Documentation

7.119.2.1 def rpki.up_down.class_elt.__init__ (*self*)

```
Initialize class_elt.
```

Definition at line 128 of file up_down.py.

7.119.2.2 def rpki.up_down.class_elt.endElement (*self*, *stack*, *name*, *text*)

```
Handle <class/> elements and their children.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 149 of file up_down.py.

7.119.2.3 def rpki.up_down.class_elt.from_resource_bag (*self*, *bag*)

```
Set resources of this class element from a resource_bag.
```

Definition at line 174 of file up_down.py.

7.119.2.4 def rpki.up_down.class_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle <class/> elements and their children.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 132 of file up_down.py.

7.119.2.5 def rpki.up_down.class_elt.to_resource_bag (*self*)

```
Build a resource_bag from from this <class/> element.
```

Definition at line 167 of file up_down.py.

7.119.2.6 def rpki.up_down.class_elt.toXML (*self*)

```
Generate a <class/> element.
```

Definition at line 157 of file up_down.py.

7.119.3 Member Data Documentation

7.119.3.1 rpki.up_down.class_elt.cert_url

Definition at line 142 of file up_down.py.

7.119.3.2 rpki.up_down.class_elt.certs

Definition at line 130 of file up_down.py.

7.119.3.3 rpki.up_down.class_elt.class_name

Definition at line 141 of file up_down.py.

7.119.3.4 rpki.up_down.class_elt.issuer = None [static]

Definition at line 126 of file up_down.py.

7.119.3.5 rpki.up_down.class_elt.resource_set_as

Definition at line 144 of file up_down.py.

7.119.3.6 rpki.up_down.class_elt.resource_set_ipv4

Definition at line 145 of file up_down.py.

7.119.3.7 rpki.up_down.class_elt.resource_set_ipv6

Definition at line 146 of file up_down.py.

7.119.3.8 rpki.up_down.class_elt.resource_set_notafter

Definition at line 147 of file up_down.py.

7.119.3.9 rpki.up_down.class_elt.suggested_sia_head

Definition at line 143 of file up_down.py.

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

- up_down.py (1873)

7.120 rpki.up_down.class_response_syntax Class Reference

Inheritance diagram for rpki.up_down.class_response_syntax:

Public Member Functions

- def __init__
- def startElement
- def toXML

Public Attributes

- classes

7.120.1 Detailed Description

```
Syntax for Up-Down protocol "list_response" and "issue_response" PDUs.
```

Definition at line 220 of file up_down.py.

7.120.2 Member Function Documentation

7.120.2.1 def rpki.up_down.class_response_syntax.__init__ (*self*)

```
Initialize class_response_syntax.
```

Definition at line 223 of file up_down.py.

7.120.2.2 def rpki.up_down.class_response_syntax.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle "list_response" and "issue_response" PDUs.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 227 of file up_down.py.

7.120.2.3 def rpki.up_down.class_response_syntax.toXML (*self*)

```
Generate payload of "list_response" and "issue_response" PDUs.
```

Definition at line 235 of file up_down.py.

7.120.3 Member Data Documentation

7.120.3.1 rpki.up_down.class_response_syntax.classes

Definition at line 225 of file up_down.py.

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

- up_down.py (1873)

7.121 rpki.up_down.cms_msg Class Reference

Inheritance diagram for rpki.up_down.cms_msg:

Static Public Attributes

- string encoding = "UTF-8"
- saxify = sax_handler.saxify
- schema = rpki.relaxng.up_down

7.121.1 Detailed Description

```
Class to hold a CMS-signed up-down PDU.
```

Definition at line 528 of file up_down.py.

7.121.2 Member Data Documentation

7.121.2.1 string rpki.up_down.cms_msg.encoding = "UTF-8" [static]

Definition at line 531 of file up_down.py.

7.121.2.2 rpki.up_down.cms_msg.saxify = sax_handler.saxify [static]

Definition at line 533 of file up_down.py.

7.121.2.3 rpki.up_down.cms_msg.schema = rpki.relaxng.up_down [static]

Definition at line 532 of file up_down.py.

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

- up_down.py (1873)

7.122 rpki.up_down.error_response_pdu Class Reference

Inheritance diagram for rpki.up_down.error_response_pdu:

Public Member Functions

- def __init__
- def check_response
- def endElement
- def toXML

Public Attributes

- description
- status

Static Public Attributes

- dictionary codes
- dictionary exceptions = { }

7.122.1 Detailed Description

```
Up-Down protocol "error_response" PDU.
```

Definition at line 389 of file up_down.py.

7.122.2 Member Function Documentation

7.122.2.1 def rpki.up_down.error_response_pdu.__init__ (*self*, *exception* = None)

```
Initialize an error_response PDU from an exception object.
```

Definition at line 405 of file up_down.py.

7.122.2.2 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 441 of file up_down.py.

7.122.2.3 def rpki.up_down.error_response_pdu.endElement (*self*, *stack*, *name*, *text*)

```
Handle "error_response" PDU.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 414 of file up_down.py.

7.122.2.4 def rpki.up_down.error_response_pdu.toXML (*self*)

```
Generate payload of "error_response" PDU.
```

Definition at line 428 of file up_down.py.

7.122.3 Member Data Documentation

7.122.3.1 dictionary rpki.up_down.error_response_pdu.codes [static]

Initial value:

```
{
    1101 : "Already processing request",
    1102 : "Version number error",
    1103 : "Unrecognised request type",
    1201 : "Request - no such resource class",
    1202 : "Request - no resources allocated in resource class",
    1203 : "Request - badly formed certificate request",
    1301 : "Revoke - no such resource class",
    1302 : "Revoke - no such key",
    2001 : "Internal Server Error - Request not performed" }
```

Definition at line 392 of file up_down.py.

7.122.3.2 rpki.up_down.error_response_pdu.description

Definition at line 412 of file up_down.py.

7.122.3.3 dictionary rpki.up_down.error_response_pdu.exceptions = {} [static]

Definition at line 403 of file up_down.py.

7.122.3.4 rpki.up_down.error_response_pdu.status

Definition at line 409 of file up_down.py.

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

- up_down.py (1873)

7.123 rpki.up_down.issue_pdu Class Reference

Inheritance diagram for rpki.up_down.issue_pdu:

Public Member Functions

- def endElement
- def query
- def serve_pdu
- def startElement

- def toXML

Public Attributes

- class_name
- pkcs10
- req_resource_set_as
- req_resource_set_ipv4
- req_resource_set_ipv6

7.123.1 Detailed Description

```
Up-Down protocol "issue" PDU.
```

Definition at line 244 of file up_down.py.

7.123.2 Member Function Documentation

7.123.2.1 def rpki.up_down.issue_pdu.endElement (*self*, *stack*, *name*, *text*)

```
Handle "issue" PDU.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 255 of file up_down.py.

7.123.2.2 def rpki.up_down.issue_pdu.query (*cls*, *parent*, *ca*, *ca_detail*)

```
Send an "issue" request to parent associated with ca.
```

Definition at line 325 of file up_down.py.

7.123.2.3 def rpki.up_down.issue_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*)

```
Serve one issue request PDU.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 268 of file up_down.py.

7.123.2.4 def rpki.up_down.issue_pdu.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle "issue" PDU.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 247 of file up_down.py.

7.123.2.5 def rpki.up_down.issue_pdu.toXML (*self*)

```
Generate payload of "issue" PDU.
```

Definition at line 261 of file up_down.py.

7.123.3 Member Data Documentation

7.123.3.1 rpki.up_down.issue_pdu.class_name

Definition at line 250 of file up_down.py.

7.123.3.2 rpki.up_down.issue_pdu.pkcs10

Definition at line 258 of file up_down.py.

7.123.3.3 rpki.up_down.issue_pdu.req_resource_set_as

Definition at line 251 of file up_down.py.

7.123.3.4 rpki.up_down.issue_pdu.req_resource_set_ipv4

Definition at line 252 of file up_down.py.

7.123.3.5 rpki.up_down.issue_pdu.req_resource_set_ipv6

Definition at line 253 of file up_down.py.

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

- up_down.py (1873)

7.124 rpki.up_down.issue_response_pdu Class Reference

Inheritance diagram for rpki.up_down.issue_response_pdu:

Public Member Functions

- def check_response

7.124.1 Detailed Description

```
Up-Down protocol "issue_response" PDU.
```

Definition at line 335 of file up_down.py.

7.124.2 Member Function Documentation

7.124.2.1 def rpki.up_down.issue_response_pdu.check_response (*self*)

```
Check whether this looks like a reasonable issue_response PDU.
XML schema should be tighter for this response.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 338 of file up_down.py.

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

- up_down.py (1873)

7.125 rpki.up_down.list_pdu Class Reference

Inheritance diagram for rpki.up_down.list_pdu:

Public Member Functions

- def query
- def serve_pdu
- def toXML

7.125.1 Detailed Description

```
Up-Down protocol "list" PDU.
```

Definition at line 181 of file up_down.py.

7.125.2 Member Function Documentation

7.125.2.1 def rpki.up_down.list_pdu.query (*cls*, *parent*)

```
Send a "list" query to parent.
```

Definition at line 216 of file up_down.py.

7.125.2.2 def rpki.up_down.list_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*)

```
Serve one "list" PDU.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 188 of file up_down.py.

7.125.2.3 def rpki.up_down.list_pdu.toXML (*self*)

```
Generate (empty) payload of "list" PDU.
```

Definition at line 184 of file up_down.py.

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

- up_down.py (1873)

7.126 rpki.up_down.list_response_pdu Class Reference

Inheritance diagram for rpki.up_down.list_response_pdu:

7.126.1 Detailed Description

```
Up-Down protocol "list_response" PDU.
```

Definition at line 239 of file up_down.py.

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

- up_down.py (1873)

7.127 rpki.up_down.message_pdu Class Reference

Inheritance diagram for rpki.up_down.message_pdu:

Public Member Functions

- def __str__
- def make_query
- def serve_error
- def serve_top_level
- def startElement
- def toXML

Public Attributes

- payload
- recipient
- sender
- type
- version

Static Public Attributes

- dictionary name2type
- tuple type2name = dict((v,k) for k,v in name2type.items())
- int version = 1

7.127.1 Detailed Description

```
Up-Down protocol message wrapper PDU.
```

Definition at line 447 of file up_down.py.

7.127.2 Member Function Documentation

7.127.2.1 def rpki.up_down.message_pdu.__str__ (*self*)

```
Convert a message PDU to a string.
```

Definition at line 484 of file up_down.py.

7.127.2.2 def rpki.up_down.message_pdu.make_query (*cls*, *payload*, *sender*, *recipient*)

```
Construct one message PDU.
```

Definition at line 507 of file up_down.py.

7.127.2.3 def rpki.up_down.message_pdu.serve_error (*self*, *exception*)

```
Generate an error_response message PDU.
```

Definition at line 497 of file up_down.py.

7.127.2.4 def rpki.up_down.message_pdu.serve_top_level (*self*, *child*)

```
Serve one message request PDU.
```

Definition at line 488 of file up_down.py.

7.127.2.5 def rpki.up_down.message_pdu.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle message PDU.

Payload of the <message/> element varies depending on the "type"
attribute, so after some basic checks we have to instantiate the
right class object to handle whatever kind of PDU this is.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 469 of file up_down.py.

7.127.2.6 def rpki.up_down.message_pdu.toXML (*self*)

```
Generate payload of message PDU.
```

Definition at line 463 of file up_down.py.

7.127.3 Member Data Documentation

7.127.3.1 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 }
```

Definition at line 452 of file up_down.py.

7.127.3.2 rpki.up_down.message_pdu.payload

Definition at line 481 of file up_down.py.

7.127.3.3 rpki.up_down.message_pdu.recipient

Definition at line 479 of file up_down.py.

7.127.3.4 rpki.up_down.message_pdu.sender

Definition at line 478 of file up_down.py.

7.127.3.5 rpki.up_down.message_pdu.type

Definition at line 480 of file up_down.py.

7.127.3.6 tuple rpki.up_down.message_pdu.type2name = dict((v,k) for k,v in name2type.items()) [static]

Definition at line 461 of file up_down.py.

7.127.3.7 rpki.up_down.message_pdu.version

Definition at line 477 of file up_down.py.

7.127.3.8 int rpki.up_down.message_pdu.version = 1 [static]

Definition at line 450 of file up_down.py.

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

- up_down.py (1873)

7.128 rpki.up_down.multi_uri Class Reference

Inheritance diagram for rpki.up_down.multi_uri:

Public Member Functions

- def __init__
- def __str__
- def rsync

7.128.1 Detailed Description

```
Container for a set of URIs.
```

Definition at line 73 of file up_down.py.

7.128.2 Member Function Documentation

7.128.2.1 def rpki.up_down.multi_uri.__init__ (*self*, *ini*)

```
Initialize a set of URIs, which includes basic some syntax checking.
```

Definition at line 76 of file up_down.py.

7.128.2.2 def rpki.up_down.multi_uri.__str__ (*self*)

```
Convert a multi_uri back to a string representation.
```

Definition at line 88 of file up_down.py.

7.128.2.3 def rpki.up_down.multi_uri.rsync (*self*)

```
Find first rsync://... URI in self.
```

Definition at line 92 of file up_down.py.

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

- up_down.py (1873)

7.129 rpki.up_down.revoke_pdu Class Reference

Inheritance diagram for rpki.up_down.revoke_pdu:

Public Member Functions

- def get_SKI
- def query
- def serve_pdu

Public Attributes

- class_name
- ski

7.129.1 Detailed Description

```
Up-Down protocol "revoke" PDU.
```

Definition at line 357 of file up_down.py.

7.129.2 Member Function Documentation

7.129.2.1 def rpki.up_down.revoke_pdu.get_SKI (*self*)

```
Convert g(SKI) encoding from PDU back to raw SKI.
```

Definition at line 360 of file up_down.py.

7.129.2.2 def rpki.up_down.revoke_pdu.query (*cls*, *ca_detail*)

```
Send a "revoke" request to parent associated with ca_detail.
```

Definition at line 375 of file up_down.py.

7.129.2.3 def rpki.up_down.revoke_pdu.serve_pdu (*self*, *q_msg*, *r_msg*, *child*)

```
Serve one revoke request PDU.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 364 of file up_down.py.

7.129.3 Member Data Documentation

7.129.3.1 rpki.up_down.revoke_pdu.class_name

Reimplemented from rpki.up_down.revoke_syntax.

Definition at line 380 of file up_down.py.

7.129.3.2 rpki.up_down.revoke_pdu.ski

Reimplemented from rpki.up_down.revoke_syntax.

Definition at line 381 of file up_down.py.

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

- up_down.py (1873)

7.130 rpki.up_down.revoke_response_pdu Class Reference

Inheritance diagram for rpki.up_down.revoke_response_pdu:

7.130.1 Detailed Description

```
Up-Down protocol "revoke_response" PDU.
```

Definition at line 384 of file up_down.py.

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

- up_down.py (1873)

7.131 rpki.up_down.revoke_syntax Class Reference

Inheritance diagram for rpki.up_down.revoke_syntax:

Public Member Functions

- def startElement
- def toXML

Public Attributes

- class_name
- ski

7.131.1 Detailed Description

```
Syntax for Up-Down protocol "revoke" and "revoke_response" PDUs.
```

Definition at line 345 of file up_down.py.

7.131.2 Member Function Documentation

7.131.2.1 def rpki.up_down.revoke_syntax.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle "revoke" PDU.
```

Reimplemented from rpki.up_down.base_elt.

Definition at line 348 of file up_down.py.

7.131.2.2 def rpki.up_down.revoke_syntax.toXML (*self*)

```
Generate payload of "revoke" PDU.
```

Definition at line 353 of file up_down.py.

7.131.3 Member Data Documentation

7.131.3.1 rpki.up_down.revoke_syntax.class_name

Reimplemented in rpki.up_down.revoke_pdu.

Definition at line 350 of file up_down.py.

7.131.3.2 rpki.up_down.revoke_syntax.ski

Reimplemented in rpki.up_down.revoke_pdu.

Definition at line 351 of file up_down.py.

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

- up_down.py (1873)

7.132 rpki.up_down.sax_handler Class Reference

Inheritance diagram for rpki.up_down.sax_handler:

Static Public Attributes

- string name = "message"
- pdu = message_pdu
- string version = "1"

7.132.1 Detailed Description

```
SAX handler for Up-Down protocol.
```

Definition at line 521 of file up_down.py.

7.132.2 Member Data Documentation

7.132.2.1 string rpki.up_down.sax_handler.name = "message" [static]

Definition at line 525 of file up_down.py.

7.132.2.2 rpki.up_down.sax_handler.pdu = message_pdu [static]

Definition at line 524 of file up_down.py.

7.132.2.3 string rpki.up_down.sax_handler.version = "1" [static]

Definition at line 526 of file up_down.py.

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

- up_down.py (1873)

7.133 rpki.x509.CMS_object Class Reference

Inheritance diagram for rpki.x509.CMS_object:

Public Member Functions

- def get_content
- def get_DER
- def get_POW
- def set_content
- def sign
- def verify

Public Attributes

- content
- DER

  DER value of this object.

- POW

Static Public Attributes

- debug_cms_certs = False

  Set this to True to log a lot of chatter about CMS certificates.

- dump_on_verify_failure = True

  Set this to True to get dumpasn1 dumps of ASN.1 on CMS verify failures.

- tuple econtent_oid = POWify_OID("id-data")
- tuple formats = ("DER", "POW")

  Formats supported in this object.

- tuple other_clear = ("content",)

  Other attributes that self.clear() should whack.

- 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.

7.133.1 Detailed Description

```
Class to hold a CMS-wrapped object.

CMS-wrapped objects are a little different from the other DER_object
types because the signed object is CMS wrapping inner content that's
also ASN.1, and due to our current minimal support for CMS we can't
just handle this as a pretty composite object.  So, for now anyway,
a CMS_object is the outer CMS wrapped object so that the usual DER
and PEM operations do the obvious things, and the inner content is
handle via separate methods.
```

Definition at line 583 of file x509.py.

7.133.2 Member Function Documentation

7.133.2.1 def rpki.x509.CMS_object.get_content (*self*)

```
Get the inner content of this CMS_object.
```

Definition at line 639 of file x509.py.

7.133.2.2 def rpki.x509.CMS_object.get_DER (*self*)

```
Get the DER value of this CMS_object.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 622 of file x509.py.

7.133.2.3 def rpki.x509.CMS_object.get_POW (*self*)

```
Get the POW value of this CMS_object.
```

Definition at line 632 of file x509.py.

7.133.2.4 def rpki.x509.CMS_object.set_content (*self*, *content*)

```
Set the (inner) content of this CMS_object, clearing the wrapper.
```

Definition at line 644 of file x509.py.

7.133.2.5 def rpki.x509.CMS_object.sign (*self*, *keypair*, *certs*, *crls* = `None`, *no_certs* = `False`)

```
Sign and wrap inner content.
```

Definition at line 718 of file x509.py.

7.133.2.6 def rpki.x509.CMS_object.verify (*self*, *ta*)

```
Verify CMS wrapper and store inner content.
```

Definition at line 649 of file x509.py.

7.133.3 Member Data Documentation

7.133.3.1 rpki.x509.CMS_object.content

Reimplemented in rpki.x509.DER_CMS_object, and rpki.x509.XML_CMS_object.

Definition at line 647 of file x509.py.

7.133.3.2 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 607 of file x509.py.

7.133.3.3 rpki.x509.CMS_object.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 628 of file x509.py.

7.133.3.4 rpki::x509.CMS_object::dump_on_verify_failure = True `[static]`

Set this to True to get dumpasn1 dumps of ASN.1 on CMS verify failures.

Definition at line 602 of file x509.py.

7.133.3.5 tuple rpki.x509.CMS_object.econtent_oid = POWify_OID("id-data") `[static]`

Reimplemented in rpki.x509.SignedManifest, rpki.x509.ROA, and rpki.x509.XML_-CMS_object.

Definition at line 597 of file x509.py.

7.133.3.6 tuple rpki.x509.CMS_object.formats = ("DER", "POW") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 595 of file x509.py.

7.133.3.7 tuple rpki.x509.CMS_object.other_clear = ("content",) [static]

Other attributes that self.clear() should whack.

Reimplemented from rpki.x509.DER_object.

Definition at line 596 of file x509.py.

7.133.3.8 rpki.x509.CMS_object.POW

Definition at line 636 of file x509.py.

7.133.3.9 rpki::x509.CMS_object::print_on_der_error = True [static]

Set this to True to log alleged DER when we have trouble parsing it, in case it's really a Perl backtrace or something.

Definition at line 620 of file x509.py.

7.133.3.10 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.

Definition at line 614 of file x509.py.

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

- x509.py (1873)

7.134 rpki.x509.CRL Class Reference

Inheritance diagram for rpki.x509.CRL:

Public Member Functions

- def generate
- def get_DER
- def get_POW
- def get_POWpkix

- def getIssuer
- def getNextUpdate
- def getThisUpdate

Public Attributes

- DER

  DER value of this object.

- POW
- POWpkix

Static Public Attributes

- tuple formats = ("DER", "POW", "POWpkix")

  Formats supported in this object.

- tuple pem_converter = PEM_converter("X509 CRL")

  PEM converter for this object.

7.134.1 Detailed Description

```
Class to hold a Certificate Revocation List.
```

Definition at line 889 of file x509.py.

7.134.2 Member Function Documentation

7.134.2.1 def rpki.x509.CRL.generate (*cls*, *keypair*, *issuer*, *serial*, *thisUpdate*, *nextUpdate*, *revokedCertificates*, *version* = `1`, *digestType* = `"sha256WithRSAEncryption"`)

Definition at line 937 of file x509.py.

7.134.2.2 def rpki.x509.CRL.get_DER (*self*)

```
Get the DER value of this CRL.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 895 of file x509.py.

7.134.2.3 def rpki.x509.CRL.get_POW (*self*)

```
Get the POW value of this CRL.
```

Definition at line 908 of file x509.py.

7.134.2.4 def rpki.x509.CRL.get_POWpkix (*self*)

```
Get the POW.pkix value of this CRL.
```

Definition at line 915 of file x509.py.

7.134.2.5 def rpki.x509.CRL.getIssuer (*self*)

```
Get issuer value of this CRL.
```

Definition at line 932 of file x509.py.

7.134.2.6 def rpki.x509.CRL.getNextUpdate (*self*)

```
Get nextUpdate value from this CRL.
```

Definition at line 928 of file x509.py.

7.134.2.7 def rpki.x509.CRL.getThisUpdate (*self*)

```
Get thisUpdate value from this CRL.
```

Definition at line 924 of file x509.py.

7.134.3 Member Data Documentation

7.134.3.1 rpki.x509.CRL.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 901 of file x509.py.

7.134.3.2 tuple rpki.x509.CRL.formats = ("DER", "POW", "POWpkix") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 892 of file x509.py.

7.134.3.3 tuple rpki.x509.CRL.pem_converter = PEM_converter("X509 CRL") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 893 of file x509.py.

7.134.3.4 rpki.x509.CRL.POW

Definition at line 912 of file x509.py.

7.134.3.5 rpki.x509.CRL.POWpkix

Definition at line 921 of file x509.py.

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

- x509.py (1873)

7.135 rpki.x509.DER_CMS_object Class Reference

Inheritance diagram for rpki.x509.DER_CMS_object:

Public Member Functions

- def decode
- def encode

Public Attributes

- content

7.135.1 Detailed Description

```
Class to hold CMS objects with DER-based content.
```

Definition at line 747 of file x509.py.

7.135.2 Member Function Documentation

7.135.2.1 def rpki.x509.DER_CMS_object.decode (*self*, *der*)

```
Decode DER and set inner content.
```

Definition at line 754 of file x509.py.

7.135.2.2 def rpki.x509.DER_CMS_object.encode (*self*)

```
Encode inner content for signing.
```

Definition at line 750 of file x509.py.

7.135.3 Member Data Documentation

7.135.3.1 rpki.x509.DER_CMS_object.content

Reimplemented from rpki.x509.CMS_object.

Definition at line 758 of file x509.py.

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

- x509.py (1873)

7.136 rpki.x509.DER_object Class Reference

Inheritance diagram for rpki.x509.DER_object:

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.

7.136.1 Detailed Description

```
Virtual class to hold a generic DER object.
```

Definition at line 76 of file x509.py.

7.136.2 Member Function Documentation

7.136.2.1 def rpki.x509.DER_object.__cmp__ (*self*, *other*)

```
Compare two DER-encoded objects.
```

Definition at line 160 of file x509.py.

7.136.2.2 def rpki.x509.DER_object.__init__ (*self*, *kw*)

```
Initialize a DER_object.
```

Definition at line 103 of file x509.py.

7.136.2.3 def rpki.x509.DER_object.clear (*self*)

```
Make this object empty.
```

Definition at line 98 of file x509.py.

7.136.2.4 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 236 of file x509.py.

7.136.2.5 def rpki.x509.DER_object.empty (*self*)

```
Test whether this object is empty.
```

Definition at line 91 of file x509.py.

7.136.2.6 def rpki.x509.DER_object.from_sql (*cls*, *x*)

```
Convert from SQL storage format.
```

Definition at line 228 of file x509.py.

7.136.2.7 def rpki.x509.DER_object.gAKI (*self*)

```
Calculate g(AKI) for this object.  Only work for subclasses
that implement get_AKI().
```

Definition at line 184 of file x509.py.

7.136.2.8 def rpki.x509.DER_object.get_3779resources (*self*)

```
Get RFC 3779 resources as rpki.resource_set objects.
Only works for subclasses that support getExtensions().
```

Definition at line 216 of file x509.py.

7.136.2.9 def rpki.x509.DER_object.get_AIA (*self*)

```
Get the SIA extension from this object.  Only works for subclasses that support getExtension().
```

Definition at line 203 of file x509.py.

7.136.2.10 def rpki.x509.DER_object.get_AKI (*self*)

```
Get the AKI extension from this object.  Only works for subclasses that support getExtension().
```

Definition at line 190 of file x509.py.

7.136.2.11 def rpki.x509.DER_object.get_Base64 (*self*)

```
Get the Base64 encoding of the DER value of this object.
```

Definition at line 152 of file x509.py.

7.136.2.12 def rpki.x509.DER_object.get_basicConstraints (*self*)

```
Get the basicConstraints extension from this object.  Only works for subclasses that support getExte
```

Definition at line 207 of file x509.py.

7.136.2.13 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 142 of file x509.py.

7.136.2.14 def rpki.x509.DER_object.get_PEM (*self*)

```
Get the PEM representation of this object.
```

Definition at line 156 of file x509.py.

7.136.2.15 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 199 of file x509.py.

7.136.2.16 def rpki.x509.DER_object.get_SKI (*self*)

```
Get the SKI extension from this object.  Only works for subclasses that support getExtension().
```

Reimplemented in rpki.x509.RSA, and rpki.x509.RSApublic.

Definition at line 195 of file x509.py.

7.136.2.17 def rpki.x509.DER_object.gSKI (*self*)

```
Calculate g(SKI) for this object.  Only work for subclasses
that implement get_SKI().
```

Definition at line 171 of file x509.py.

7.136.2.18 def rpki.x509.DER_object.hAKI (*self*)

```
Return hexadecimal string representation of AKI for this
object.  Only work for subclasses that implement get_AKI().
```

Definition at line 177 of file x509.py.

7.136.2.19 def rpki.x509.DER_object.hSKI (*self*)

```
Return hexadecimal string representation of SKI for this
object.  Only work for subclasses that implement get_SKI().
```

Definition at line 164 of file x509.py.

7.136.2.20 def rpki.x509.DER_object.is_CA (*self*)

```
Return True if and only if object has the basicConstraints extension and its cA value is true.
```

Definition at line 211 of file x509.py.

7.136.2.21 def rpki.x509.DER_object.set (*self*, *kw*)

```
Set this object by setting one of its known formats.

This method only allows one to set one format at a time.
Subsequent calls will clear the object first.  The point of all
this is to let the object's internal converters handle mustering
the object into whatever format you need at the moment.
```

Definition at line 109 of file x509.py.

7.136.2.22 def rpki.x509.DER_object.to_sql (*self*)

```
Convert to SQL storage format.
```

Definition at line 232 of file x509.py.

7.136.3 Member Data Documentation

7.136.3.1 rpki::x509.DER_object::DER

DER value of this object.

Reimplemented in rpki.x509.X509, rpki.x509.PKCS10, rpki.x509.RSA, rpki.x509.RSApublic, rpki.x509.CMS_object, and rpki.x509.CRL.

Definition at line 125 of file x509.py.

7.136.3.2 tuple rpki.x509.DER_object.formats = ("DER",) [static]

Formats supported in this object.

Reimplemented in rpki.x509.X509, rpki.x509.PKCS10, rpki.x509.RSA, rpki.x509.RSApublic, rpki.x509.CMS_object, and rpki.x509.CRL.

Definition at line 80 of file x509.py.

7.136.3.3 tuple rpki.x509.DER_object.other_clear = () [static]

Other attributes that self.clear() should whack.

Reimplemented in rpki.x509.CMS_object.

Definition at line 86 of file x509.py.

7.136.3.4 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.SignedManifest, rpki.x509.ROA, and rpki.x509.CRL.

Definition at line 83 of file x509.py.

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

- x509.py (1873)

7.137 rpki.x509.PEM_converter Class Reference

Inheritance diagram for rpki.x509.PEM_converter:

Public Member Functions

- def __init__
- def looks_like_PEM
- def to_DER
- def to_PEM

Public Attributes

- b
- e

7.137.1 Detailed Description

```
Convert between DER and PEM encodings for various kinds of ASN.1 data.
```

Definition at line 43 of file x509.py.

7.137.2 Member Function Documentation

7.137.2.1 def rpki.x509.PEM_converter.__init__ (*self*, *kind*)

```
Initialize PEM_converter.
```

Definition at line 46 of file x509.py.

7.137.2.2 def rpki.x509.PEM_converter.looks_like_PEM (*self*, *text*)

```
Guess whether text looks like a PEM encoding.
```

Definition at line 51 of file x509.py.

7.137.2.3 def rpki.x509.PEM_converter.to_DER (*self*, *pem*)

```
Convert from PEM to DER.
```

Definition at line 56 of file x509.py.

7.137.2.4 def rpki.x509.PEM_converter.to_PEM (*self*, *der*)

```
Convert from DER to PEM.
```

Definition at line 67 of file x509.py.

7.137.3 Member Data Documentation

7.137.3.1 rpki.x509.PEM_converter.b

Definition at line 48 of file x509.py.

7.137.3.2 rpki.x509.PEM_converter.e

Definition at line 49 of file x509.py.

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

- x509.py (1873)

7.138 rpki.x509.PKCS10 Class Reference

Inheritance diagram for rpki.x509.PKCS10:

Public Member Functions

- def check_valid_rpki
- def create
- def create_ca
- def get_DER

- def get_POWpkix
- def getPublicKey

Public Attributes

- DER

  DER value of this object.

- POWpkix

Static Public Attributes

- tuple formats = ("DER", "POWpkix")

  Formats supported in this object.

- tuple pem_converter = PEM_converter("CERTIFICATE REQUEST")

  PEM converter for this object.

7.138.1 Detailed Description

```
Class to hold a PKCS #10 request.
```

Definition at line 402 of file x509.py.

7.138.2 Member Function Documentation

7.138.2.1 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 431 of file x509.py.

7.138.2.2 def rpki.x509.PKCS10.create (*cls*, *keypair*, *exts* = None)

```
Create a new request for a given keypair, including given extensions.
```

Definition at line 488 of file x509.py.

7.138.2.3 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 477 of file x509.py.

7.138.2.4 def rpki.x509.PKCS10.get_DER (*self*)

```
Get the DER value of this certification request.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 408 of file x509.py.

7.138.2.5 def rpki.x509.PKCS10.get_POWpkix (*self*)

```
Get the POW.pkix value of this certification request.
```

Definition at line 418 of file x509.py.

7.138.2.6 def rpki.x509.PKCS10.getPublicKey (*self*)

```
Extract the public key from this certification request.
```

Definition at line 427 of file x509.py.

7.138.3 Member Data Documentation

7.138.3.1 rpki.x509.PKCS10.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 414 of file x509.py.

7.138.3.2 tuple rpki.x509.PKCS10.formats = ("DER", "POWpkix") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 405 of file x509.py.

7.138.3.3 tuple rpki.x509.PKCS10.pem_converter = PEM_converter("CERTIFICATE REQUEST") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 406 of file x509.py.

7.138.3.4 rpki.x509.PKCS10.POWpkix

Definition at line 424 of file x509.py.

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

- x509.py (1873)

7.139 rpki.x509.ROA Class Reference

Inheritance diagram for rpki.x509.ROA:

Public Member Functions

- def build

Static Public Attributes

- content_class = rpki.roa.RouteOriginAttestation
- tuple econtent_oid = POWify_OID("id-ct-routeOriginAttestation")
- tuple pem_converter = PEM_converter("ROUTE ORIGIN ATTESTATION")

  PEM converter for this object.

7.139.1 Detailed Description

```
Class to hold a signed ROA.
```

Definition at line 796 of file x509.py.

7.139.2 Member Function Documentation

7.139.2.1 def rpki.x509.ROA.build (*cls*, *as_number*, *ipv4*, *ipv6*, *keypair*, *certs*, *version* = 0)

```
Build a ROA.
```

Definition at line 804 of file x509.py.

7.139.3 Member Data Documentation

7.139.3.1 rpki.x509.ROA.content_class = rpki.roa.RouteOriginAttestation [static]

Definition at line 800 of file x509.py.

7.139.3.2 tuple rpki.x509.ROA.econtent_oid = POWify_OID("id-ct-routeOriginAttestation") [static]

Reimplemented from rpki.x509.CMS_object.

Definition at line 801 of file x509.py.

7.139.3.3 tuple rpki.x509.ROA.pem_converter = PEM_converter("ROUTE ORIGIN ATTESTATION") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 799 of file x509.py.

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

- x509.py (1873)

7.140 rpki.x509.RSA Class Reference

Inheritance diagram for rpki.x509.RSA:

Public Member Functions

- def generate
- def get_DER
- def get_POW
- def get_public_DER
- def get_RSApublic
- def get_SKI
- def get_tlslite

Public Attributes

- DER

  DER value of this object.

- POW
- tlslite

Static Public Attributes

- tuple formats = ("DER", "POW", "tlslite")

  Formats supported in this object.

- tuple pem_converter = PEM_converter("RSA PRIVATE KEY")

  PEM converter for this object.

7.140.1 Detailed Description

```
Class to hold an RSA key pair.
```

Definition at line 500 of file x509.py.

7.140.2 Member Function Documentation

7.140.2.1 def rpki.x509.RSA.generate (*self*, *keylength* = 2048)

```
Generate a new keypair.
```

Definition at line 530 of file x509.py.

7.140.2.2 def rpki.x509.RSA.get_DER (*self*)

```
Get the DER value of this keypair.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 506 of file x509.py.

7.140.2.3 def rpki.x509.RSA.get_POW (*self*)

```
Get the POW value of this keypair.
```

Definition at line 516 of file x509.py.

7.140.2.4 def rpki.x509.RSA.get_public_DER (*self*)

```
Get the DER encoding of the public key from this keypair.
```

Definition at line 535 of file x509.py.

7.140.2.5 def rpki.x509.RSA.get_RSApublic (*self*)

```
Convert the public key of this keypair into a RSApublic object.
```

Definition at line 543 of file x509.py.

7.140.2.6 def rpki.x509.RSA.get_SKI (*self*)

```
Calculate the SKI of this keypair.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 539 of file x509.py.

7.140.2.7 def rpki.x509.RSA.get_tlslite (*self*)

```
Get the tlslite value of this keypair.
```

Definition at line 523 of file x509.py.

7.140.3 Member Data Documentation

7.140.3.1 rpki.x509.RSA.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 512 of file x509.py.

7.140.3.2 tuple rpki.x509.RSA.formats = ("DER", "POW", "tlslite") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 503 of file x509.py.

7.140.3.3 tuple rpki.x509.RSA.pem_converter = PEM_converter("RSA PRIVATE KEY") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 504 of file x509.py.

7.140.3.4 rpki.x509.RSA.POW

Definition at line 520 of file x509.py.

7.140.3.5 rpki.x509.RSA.tlslite

Definition at line 527 of file x509.py.

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

- x509.py (1873)

7.141 rpki.x509.RSApublic Class Reference

Inheritance diagram for rpki.x509.RSApublic:

Public Member Functions

- def get_DER
- def get_POW
- def get_SKI

Public Attributes

- DER
  DER value of this object.
- POW

Static Public Attributes

- tuple formats = ("DER", "POW")
  Formats supported in this object.
- tuple pem_converter = PEM_converter("RSA PUBLIC KEY")
  PEM converter for this object.

7.141.1 Detailed Description

```
Class to hold an RSA public key.
```

Definition at line 547 of file x509.py.

7.141.2 Member Function Documentation

7.141.2.1 def rpki.x509.RSApublic.get_DER (*self*)

```
Get the DER value of this public key.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 553 of file x509.py.

7.141.2.2 def rpki.x509.RSApublic.get_POW (*self*)

```
Get the POW value of this public key.
```

Definition at line 563 of file x509.py.

7.141.2.3 def rpki.x509.RSApublic.get_SKI (*self*)

```
Calculate the SKI of this public key.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 570 of file x509.py.

7.141.3 Member Data Documentation

7.141.3.1 rpki.x509.RSApublic.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 559 of file x509.py.

7.141.3.2 tuple rpki.x509.RSApublic.formats = ("DER", "POW") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 550 of file x509.py.

7.141.3.3 tuple rpki.x509.RSApublic.pem_converter = PEM_converter("RSA PUBLIC KEY") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 551 of file x509.py.

7.141.3.4 rpki.x509.RSApublic.POW

Definition at line 567 of file x509.py.

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

- x509.py (1873)

7.142 rpki.x509.SignedManifest Class Reference

Inheritance diagram for rpki.x509.SignedManifest:

Public Member Functions

- def build
- def getNextUpdate
- def getThisUpdate

Static Public Attributes

- content_class = rpki.manifest.Manifest
- tuple econtent_oid = POWify_OID("id-ct-rpkiManifest")
- tuple pem_converter = PEM_converter("RPKI MANIFEST")

  PEM converter for this object.

7.142.1 Detailed Description

```
Class to hold a signed manifest.
```

Definition at line 760 of file x509.py.

7.142.2 Member Function Documentation

7.142.2.1 def rpki.x509.SignedManifest.build (*cls*, *serial*, *thisUpdate*, *nextUpdate*, *names_and_objs*, *keypair*, *certs*, *version* = 0)

```
Build a signed manifest.
```

Definition at line 776 of file x509.py.

7.142.2.2 def rpki.x509.SignedManifest.getNextUpdate (*self*)

```
Get nextUpdate value from this manifest.
```

Definition at line 771 of file x509.py.

7.142.2.3 def rpki.x509.SignedManifest.getThisUpdate (*self*)

```
Get thisUpdate value from this manifest.
```

Definition at line 767 of file x509.py.

7.142.3 Member Data Documentation

7.142.3.1 rpki.x509.SignedManifest.content_class = rpki.manifest.Manifest [static]

Definition at line 764 of file x509.py.

7.142.3.2 tuple rpki.x509.SignedManifest.econtent_oid = POWify_OID("id-ct-rpkiManifest") [static]

Reimplemented from rpki.x509.CMS_object.

Definition at line 765 of file x509.py.

7.142.3.3 tuple rpki.x509.SignedManifest.pem_converter = PEM_converter("RPKI MANIFEST") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 763 of file x509.py.

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

- x509.py (1873)

7.143 rpki.x509.X509 Class Reference

Inheritance diagram for rpki.x509.X509:

Public Member Functions

- def get_DER
- def get_POW
- def get_POWpkix
- def get_tlslite

- 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
- tlslite

Static Public Attributes

- tuple formats = ("DER", "POW", "POWpkix", "tlslite")

  Formats supported in this object.

- tuple pem_converter = PEM_converter("CERTIFICATE")

  PEM converter for this object.

7.143.1 Detailed Description

```
X.509 certificates.

This class is designed to hold all the different representations of
X.509 certs we're using and convert between them.  X.509 support in
Python a nasty maze of half-cooked stuff (except perhaps for
cryptlib, which is just different).  Users of this module should not
have to care about this implementation nightmare.
```

Definition at line 255 of file x509.py.

7.143.2 Member Function Documentation

7.143.2.1 def rpki.x509.X509.get_DER (*self*)

```
Get the DER value of this certificate.
```

Reimplemented from rpki.x509.DER_object.

Definition at line 268 of file x509.py.

7.143.2.2 def rpki.x509.X509.get_POW (*self*)

```
Get the POW value of this certificate.
```

Definition at line 287 of file x509.py.

7.143.2.3 def rpki.x509.X509.get_POWpkix (*self*)

```
Get the POW.pkix value of this certificate.
```

Definition at line 294 of file x509.py.

7.143.2.4 def rpki.x509.X509.get_tlslite (*self*)

```
Get the tlslite value of this certificate.
```

Definition at line 303 of file x509.py.

7.143.2.5 def rpki.x509.X509.getIssuer (*self*)

```
Get the issuer of this certificate.
```

Definition at line 312 of file x509.py.

7.143.2.6 def rpki.x509.X509.getNotAfter (*self*)

```
Get the expiration time of this certificate.
```

Definition at line 324 of file x509.py.

7.143.2.7 def rpki.x509.X509.getNotBefore (*self*)

```
Get the inception time of this certificate.
```

Definition at line 320 of file x509.py.

7.143.2.8 def rpki.x509.X509.getPublicKey (*self*)

```
Extract the public key from this certificate.
```

Definition at line 332 of file x509.py.

7.143.2.9 def rpki.x509.X509.getSerial (*self*)

```
Get the serial number of this certificate.
```

Definition at line 328 of file x509.py.

7.143.2.10 def rpki.x509.X509.getSubject (*self*)

```
Get the subject of this certificate.
```

Definition at line 316 of file x509.py.

7.143.2.11 def rpki.x509.X509.issue (*self*, *keypair*, *subject_key*, *serial*, *sia*, *aia*, *crldp*, *notAfter*, *cn* = `None`, *resources* = `None`, *is_ca* = `True`)

```
Issue a certificate.
```

Definition at line 336 of file x509.py.

7.143.2.12 def rpki.x509.X509.normalize_chain (*cls*, *chain*)

```
Normalize a chain of certificates into a tuple of X509 objects.
Given all the glue certificates needed for BPKI cross
certification, it's easiest to allow sloppy arguments to the HTTPS
and CMS validation methods and provide a single method that
normalizes the allowed cases.  So this method allows X509, None,
lists, and tuples, and returns a tuple of X509 objects.
```

Definition at line 390 of file x509.py.

7.143.3 Member Data Documentation

7.143.3.1 rpki.x509.X509.DER

DER value of this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 274 of file x509.py.

7.143.3.2 tuple rpki.x509.X509.formats = ("DER", "POW", "POWpkix", "tlslite") [static]

Formats supported in this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 265 of file x509.py.

7.143.3.3 tuple rpki.x509.X509.pem_converter = PEM_converter("CERTIFICATE") [static]

PEM converter for this object.

Reimplemented from rpki.x509.DER_object.

Definition at line 266 of file x509.py.

7.143.3.4 rpki.x509.X509.POW

Definition at line 291 of file x509.py.

7.143.3.5 rpki.x509.X509.POWpkix

Definition at line 300 of file x509.py.

7.143.3.6 rpki.x509.X509.tlslite

Definition at line 309 of file x509.py.

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

- x509.py (1873)

7.144 rpki.x509.XML_CMS_object Class Reference

Inheritance diagram for rpki.x509.XML_CMS_object:

Public Member Functions

- def decode
- def dump_to_disk
- def encode
- def pretty_print_content
- def schema_check
- def unwrap
- def wrap

Public Attributes

- content

Static Public Attributes

- dump_inbound_cms = None
- 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")

7.144.1 Detailed Description

```
Class to hold CMS-wrapped XML protocol data.
```

Definition at line 815 of file x509.py.

7.144.2 Member Function Documentation

7.144.2.1 def rpki.x509.XML_CMS_object.decode (*self*, *xml*)

```
Decode XML and set inner content.
```

Definition at line 838 of file x509.py.

7.144.2.2 def rpki.x509.XML_CMS_object.dump_to_disk (*self*, *prefix*)

```
Write DER of current message to disk, for debugging.
```

Definition at line 854 of file x509.py.

7.144.2.3 def rpki.x509.XML_CMS_object.encode (*self*)

```
Encode inner content for signing.
```

Definition at line 834 of file x509.py.

7.144.2.4 def rpki.x509.XML_CMS_object.pretty_print_content (*self*)

```
Pretty print XML content of this message.
```

Definition at line 842 of file x509.py.

7.144.2.5 def rpki.x509.XML_CMS_object.schema_check (*self*)

```
Handle XML RelaxNG schema check.
```

Definition at line 846 of file x509.py.

7.144.2.6 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 876 of file x509.py.

7.144.2.7 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 861 of file x509.py.

7.144.3 Member Data Documentation

7.144.3.1 rpki.x509.XML_CMS_object.content

Reimplemented from rpki.x509.CMS_object.

Definition at line 840 of file x509.py.

7.144.3.2 rpki.x509.XML_CMS_object.dump_inbound_cms = None [static]

Definition at line 832 of file x509.py.

7.144.3.3 rpki::x509.XML_CMS_object::dump_outbound_cms = None [static]

If set, we write all outbound XML-CMS PDUs to disk, for debugging.

If set, we write all inbound XML-CMS PDUs to disk, for debugging.

Value of this variable is prefix portion of filename, tail will be a timestamp.

Definition at line 825 of file x509.py.

7.144.3.4 tuple rpki.x509.XML_CMS_object.econtent_oid = POWify_OID("id-ct-xml") [static]

Reimplemented from rpki.x509.CMS_object.

Definition at line 818 of file x509.py.

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

- x509.py (1873)

7.145 rpki.xml_utils.base_elt Class Reference

Inheritance diagram for rpki.xml_utils.base_elt:

Public Member Functions

- def __str__
- def endElement
- def make_b64elt
- def make_elt
- def make_pdu
- def read_attrs
- def startElement
- def toXML

Static Public Attributes

- tuple attributes = ()

XML attributes for this element.

- tuple booleans = ()

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

- tuple elements = ()

  XML elements contained by this element.

7.145.1 Detailed Description

```
Virtual base class for XML message elements.  The left-right and
publication protocols use this.  At least for now, the up-down
protocol does not, due to different design assumptions.
```

Definition at line 101 of file xml_utils.py.

7.145.2 Member Function Documentation

7.145.2.1 def rpki.xml_utils.base_elt.__str__ (*self*)

```
Convert a base_elt object to string format.
```

Definition at line 163 of file xml_utils.py.

7.145.2.2 def rpki.xml_utils.base_elt.endElement (*self*, *stack*, *name*, *text*)

```
Default endElement() handler: just pop the stack.
```

Reimplemented in rpki.left_right.child_elt, rpki.publication.client_elt, rpki.publication.publication_object_elt, and rpki.xml_utils.data_elt.

Definition at line 125 of file xml_utils.py.

7.145.2.3 def rpki.xml_utils.base_elt.make_b64elt (*self*, *elt*, *name*, *value* = None)

```
Constructor for Base64-encoded subelement.
```

Definition at line 156 of file xml_utils.py.

7.145.2.4 def rpki.xml_utils.base_elt.make_elt (*self*)

```
XML element constructor.
```

Definition at line 144 of file xml_utils.py.

7.145.2.5 def rpki.xml_utils.base_elt.make_pdu (*cls*, *kargs*)

```
Generic PDU constructor.
```

Definition at line 168 of file xml_utils.py.

7.145.2.6 def rpki.xml_utils.base_elt.read_attrs (*self*, *attrs*)

```
Template-driven attribute reader.
```

Definition at line 134 of file xml_utils.py.

7.145.2.7 def rpki.xml_utils.base_elt.startElement (*self*, *stack*, *name*, *attrs*)

```
Default startElement() handler: just process attributes.
```

Reimplemented in rpki.left_right.route_origin_elt, rpki.left_right.list_resources_elt, and rpki.publication.config_elt.

Definition at line 119 of file xml_utils.py.

7.145.2.8 def rpki.xml_utils.base_elt.toXML (*self*)

```
Default toXML() element generator.
```

Reimplemented in rpki.left_right.list_resources_elt, rpki.publication.publication_object_elt, and rpki.xml_utils.data_elt.

Definition at line 130 of file xml_utils.py.

7.145.3 Member Data Documentation

7.145.3.1 rpki::xml_utils.base_elt::attributes = () [static]

XML attributes for this element.

Reimplemented in rpki.left_right.self_elt, rpki.left_right.bsc_elt, rpki.left_right.parent_elt, rpki.left_right.child_elt, rpki.left_right.repository_elt, rpki.left_right.route_origin_elt, rpki.left_right.list_resources_elt, rpki.left_right.report_error_elt, rpki.publication.config_elt, rpki.publication.client_elt, rpki.publication.publication_object_elt, and rpki.publication.report_error_elt.

Definition at line 109 of file xml_utils.py.

7.145.3.2 rpki::xml_utils.base_elt::booleans = () [static]

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

Reimplemented in rpki.left_right.self_elt, rpki.left_right.bsc_elt, rpki.left_right.parent_elt, rpki.left_right.child_elt, and rpki.left_right.route_origin_elt.

Definition at line 117 of file xml_utils.py.

7.145.3.3 rpki::xml_utils.base_elt::elements = () [static]

XML elements contained by this element.

Reimplemented in rpki.left_right.self_elt, rpki.left_right.bsc_elt, rpki.left_right.parent_elt, rpki.left_right.child_elt, rpki.left_right.repository_elt, rpki.publication.config_elt, and rpki.publication.client_elt.

Definition at line 113 of file xml_utils.py.

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

- xml_utils.py (1873)

7.146 rpki.xml_utils.data_elt Class Reference

Inheritance diagram for rpki.xml_utils.data_elt:

Public Member Functions

- def endElement
- def make_reply
- def make_reply_clone_hook
- def serve_create
- def serve_destroy
- def serve_dispatch
- def serve_get
- def serve_list
- def serve_post_save_hook

- def serve_pre_save_hook
- def serve_set
- def toXML
- def unimplemented_control

7.146.1 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 177 of file xml_utils.py.

7.146.2 Member Function Documentation

7.146.2.1 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 183 of file xml_utils.py.

7.146.2.2 def rpki.xml_utils.data_elt.make_reply (*self*, *r_pdu* = `None`)

```
Construct a reply PDU.
```

Definition at line 206 of file xml_utils.py.

7.146.2.3 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 219 of file xml_utils.py.

7.146.2.4 def rpki.xml_utils.data_elt.serve_create (*self*, *r_msg*)

```
Handle a create action.
```

Definition at line 231 of file xml_utils.py.

7.146.2.5 def rpki.xml_utils.data_elt.serve_destroy (*self*, *r_msg*)

```
Handle a destroy action.
```

Definition at line 266 of file xml_utils.py.

7.146.2.6 def rpki.xml_utils.data_elt.serve_dispatch (*self*, *r_msg*)

```
Action dispatch handler.
```

Definition at line 272 of file xml_utils.py.

7.146.2.7 def rpki.xml_utils.data_elt.serve_get (*self*, *r_msg*)

```
Handle a get action.
```

Definition at line 254 of file xml_utils.py.

7.146.2.8 def rpki.xml_utils.data_elt.serve_list (*self*, *r_msg*)

```
Handle a list action for non-self objects.
```

Definition at line 260 of file xml_utils.py.

7.146.2.9 def rpki.xml_utils.data_elt.serve_post_save_hook (*self*, *q_pdu*, *r_pdu*)

```
Overridable hook.
```

Reimplemented in rpki.left_right.self_elt, rpki.left_right.parent_elt, rpki.left_right.child_elt, rpki.left_right.route_origin_elt, and rpki.publication.client_elt.

Definition at line 227 of file xml_utils.py.

7.146.2.10 def rpki.xml_utils.data_elt.serve_pre_save_hook (*self*, *q_pdu*, *r_pdu*)

```
Overridable hook.
```

Reimplemented in rpki.left_right.bsc_elt.

Definition at line 223 of file xml_utils.py.

7.146.2.11 def rpki.xml_utils.data_elt.serve_set (*self*, *r_msg*)

```
Handle a set action.
```

Reimplemented in rpki.publication.config_elt.

Definition at line 240 of file xml_utils.py.

7.146.2.12 def rpki.xml_utils.data_elt.toXML (*self*)

```
Default element generator for SQL-based objects.  This assumes
that sub-elements are Base64-encoded DER objects.
```

Reimplemented from rpki.xml_utils.base_elt.

Definition at line 195 of file xml_utils.py.

7.146.2.13 def rpki.xml_utils.data_elt.unimplemented_control (*self*, *controls*)

```
Uniform handling for unimplemented control operations.
```

Reimplemented in rpki.left_right.data_elt.

Definition at line 283 of file xml_utils.py.

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

- xml_utils.py (1873)

7.147 rpki.xml_utils.msg Class Reference

Inheritance diagram for rpki.xml_utils.msg:

Public Member Functions

- def __str__
- def endElement
- def startElement
- def toXML

Public Attributes

- type
- version

7.147.1 Detailed Description

```
Generic top-level PDU.
```

Definition at line 289 of file xml_utils.py.

7.147.2 Member Function Documentation

7.147.2.1 def rpki.xml_utils.msg.__str__ (*self*)

```
Convert msg object to string.
```

Definition at line 309 of file xml_utils.py.

7.147.2.2 def rpki.xml_utils.msg.endElement (*self*, *stack*, *name*, *text*)

```
Handle top-level PDU.
```

Definition at line 303 of file xml_utils.py.

7.147.2.3 def rpki.xml_utils.msg.startElement (*self*, *stack*, *name*, *attrs*)

```
Handle top-level PDU.
```

Definition at line 292 of file xml_utils.py.

7.147.2.4 def rpki.xml_utils.msg.toXML (*self*)

```
Generate top-level PDU.
```

Definition at line 313 of file xml_utils.py.

7.147.3 Member Data Documentation

7.147.3.1 rpki.xml_utils.msg.type

Definition at line 296 of file xml_utils.py.

7.147.3.2 rpki.xml_utils.msg.version

Reimplemented in rpki.left_right.msg, and rpki.publication.msg.

Definition at line 295 of file xml_utils.py.

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

- xml_utils.py (1873)

7.148 rpki.xml_utils.sax_handler Class Reference

Inheritance diagram for rpki.xml_utils.sax_handler:

Public Member Functions

- def __init__
- def characters
- def create_top_level
- def endElement
- def endElementNS
- def saxify
- def startElement
- def startElementNS

Public Attributes

- result
- stack
- text

7.148.1 Detailed Description

```
SAX handler for RPKI protocols.

This class provides some basic amenities for parsing protocol XML of
the kind we use in the RPKI protocols, including whacking all the
protocol element text into US-ASCII, simplifying accumulation of
text fields, and hiding some of the fun relating to XML namespaces.

General assumption: by the time this parsing code gets invoked, the
XML has already passed RelaxNG validation, so we only have to check
for errors that the schema can't catch, and we don't have to play as
many XML namespace games.
```

Definition at line 22 of file xml_utils.py.

7.148.2 Member Function Documentation

7.148.2.1 def rpki.xml_utils.sax_handler.__init__ (*self*)

```
Initialize SAX handler.
```

Definition at line 36 of file xml_utils.py.

7.148.2.2 def rpki.xml_utils.sax_handler.characters (*self*, *content*)

```
Accumulate a chuck of element content (text).
```

Definition at line 49 of file xml_utils.py.

7.148.2.3 def rpki.xml_utils.sax_handler.create_top_level (*self*, *name*, *attrs*)

```
Handle top-level PDU for this protocol.
```

Definition at line 96 of file xml_utils.py.

7.148.2.4 def rpki.xml_utils.sax_handler.endElement (*self*, *name*)

```
Handle endElement() events.

Mostly this means handling any accumulated element text.
```

Definition at line 79 of file xml_utils.py.

7.148.2.5 def rpki.xml_utils.sax_handler.endElementNS (*self*, *name*, *qname*)

```
Redirect endElementNS() events to endElement().
```

Definition at line 45 of file xml_utils.py.

7.148.2.6 def rpki.xml_utils.sax_handler.saxify (*cls*, *elt*)

```
Create a one-off SAX parser, parse an ETree, return the result.
```

Definition at line 89 of file xml_utils.py.

7.148.2.7 def rpki.xml_utils.sax_handler.startElement (*self*, *name*, *attrs*)

```
Handle startElement() events.

We maintain a stack of nested elements under construction so that
we can feed events directly to the current element rather than
having to pass them through all the nesting elements.

If the stack is empty, this event is for the outermost element, so
we call a virtual method to create the corresponding object and
that's the object we'll be returning as our final result.
```

Definition at line 53 of file xml_utils.py.

7.148.2.8 def rpki.xml_utils.sax_handler.startElementNS (*self*, *name*, *qname*, *attrs*)

```
Redirect startElementNS() events to startElement().
```

Definition at line 41 of file xml_utils.py.

7.148.3 Member Data Documentation

7.148.3.1 rpki.xml_utils.sax_handler.result

Definition at line 75 of file xml_utils.py.

7.148.3.2 rpki.xml_utils.sax_handler.stack

Definition at line 39 of file xml_utils.py.

7.148.3.3 rpki.xml_utils.sax_handler.text

Definition at line 38 of file xml_utils.py.

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

- xml_utils.py (1873)

7.149 Sequence Class Reference

Inheritance diagram for Sequence:

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

- roa.py (1873)

7.150 SequenceOf Class Reference

Inheritance diagram for SequenceOf:

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

- roa.py (1873)

7.151 Checker Class Reference

Inheritance diagram for Checker:

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

- https.py (1873)

7.152 HTTPTLSConnection Class Reference

Inheritance diagram for HTTPTLSConnection:

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

- https.py (1873)

7.153 TLSSocketServerMixIn Class Reference

Inheritance diagram for TLSSocketServerMixIn:

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

- https.py (1873)

7.154 ContentHandler Class Reference

Inheritance diagram for ContentHandler:

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

- xml_utils.py (1873)

8 File Documentation

8.1 __init__.py File Reference

Namespaces

- namespace rpki

8.2 config.py File Reference

Namespaces

- namespace rpki.config

Classes

- class rpki.config.parser

8.3 exceptions.py File Reference

Namespaces

- namespace rpki.exceptions

Classes

- class rpki.exceptions.BadClassNameSyntax
- class rpki.exceptions.BadContactURL
- class rpki.exceptions.BadIRDBReply
- class rpki.exceptions.BadIssueResponse
- class rpki.exceptions.BadPKCS10
- class rpki.exceptions.BadQuery
- class rpki.exceptions.BadSender
- class rpki.exceptions.BadStatusCode
- class rpki.exceptions.BadURISyntax
- class rpki.exceptions.BSCNotFound
- class rpki.exceptions.ChildNotFound
- class rpki.exceptions.ClassNameMismatch
- class rpki.exceptions.CMSCRLNotSet
- class rpki.exceptions.CMSVerificationFailed
- class rpki.exceptions.DBConsistancyError

- class rpki.exceptions.DERObjectConversionError
- class rpki.exceptions.EmptyPEM
- class rpki.exceptions.HTTPRequestFailed
- class rpki.exceptions.MissingCMSCRL
- class rpki.exceptions.MissingCMSEEcert
- class rpki.exceptions.MultipleTLSEECert
- class rpki.exceptions.MustBePrefix
- class rpki.exceptions.NotACertificateChain
- class rpki.exceptions.NotFound
- class rpki.exceptions.NotImplementedYet
- class rpki.exceptions.NotInDatabase
- class rpki.exceptions.ReceivedTLSCACert
- class rpki.exceptions.RPKI_Exception
- class rpki.exceptions.ServerShuttingDown
- class rpki.exceptions.SKIMismatch
- class rpki.exceptions.SubprocessError
- class rpki.exceptions.TLSValidationError
- class rpki.exceptions.UnexpectedCMSCerts
- class rpki.exceptions.UnexpectedCMSCRLs
- class rpki.exceptions.UnparsableCMSDER
- class rpki.exceptions.UpstreamError
- class rpki.exceptions.WrongEContentType

8.4 https.py File Reference

Namespaces

- namespace rpki.https

Classes

- class rpki.https.Checker
- class rpki.https.httpsClient
- class rpki.https.httpsServer
- class rpki.https.requestHandler

Functions

- def rpki::https.build_https_ta_cache
- def rpki::https.client
- def rpki::https.server
- def rpki::https.tlslite_certChain

Variables

- rpki::https.debug_tls_certs = False
- rpki::https.disable_tls_certificate_validation_exceptions = False
- string rpki::https.rpki_content_type = "application/x-rpki"

8.5 ipaddrs.py File Reference

Namespaces

- namespace rpki.ipaddrs

Classes

- class rpki.ipaddrs.v4addr
- class rpki.ipaddrs.v6addr

8.6 left_right.py File Reference

Namespaces

- namespace rpki.left_right

Classes

- class rpki.left_right.bsc_elt
- class rpki.left_right.child_elt
- class rpki.left_right.cms_msg
- class rpki.left_right.data_elt
- class rpki.left_right.left_right_namespace
- class rpki.left_right.list_resources_elt
- class rpki.left_right.msg
- class rpki.left_right.parent_elt
- class rpki.left_right.report_error_elt
- class rpki.left_right.repository_elt
- class rpki.left_right.route_origin_elt
- class rpki.left_right.sax_handler
- class rpki.left_right.self_elt

Variables

- rpki::left_right.enforce_strict_up_down_xml_sender = False

8.7 log.py File Reference

Namespaces

- namespace rpki.log

Classes

- class rpki.log.logger

Functions

- def rpki::log.init
- def rpki::log.set_trace
- def rpki::log.trace

Variables

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

  Whether call tracing is enabled.

- tuple rpki::log.error = logger(syslog.LOG_ERR)
- tuple rpki::log.info = logger(syslog.LOG_INFO)
- tuple rpki::log.note = logger(syslog.LOG_NOTICE)
- tuple rpki::log.warn = logger(syslog.LOG_WARNING)

8.8 manifest.py File Reference

Namespaces

- namespace rpki.manifest

Classes

- class rpki.manifest.FileAndHash
- class rpki.manifest.FilesAndHashes
- class rpki.manifest.Manifest

8.9 oids.py File Reference

Namespaces

- namespace 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.

8.10 pubd.py File Reference

Namespaces

- namespace pubd

Classes

- class pubd.pubd_context

Functions

- def pubd.main

Variables

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

8.11 publication.py File Reference

Namespaces

- namespace rpki.publication

Classes

- class rpki.publication.certificate_elt
- class rpki.publication.client_elt
- class rpki.publication.cms_msg
- class rpki.publication.config_elt
- class rpki.publication.control_elt
- class rpki.publication.crl_elt
- class rpki.publication.manifest_elt
- class rpki.publication.msg
- class rpki.publication.publication_namespace
- class rpki.publication.publication_object_elt
- class rpki.publication.report_error_elt
- class rpki.publication.roa_elt
- class rpki.publication.sax_handler

Variables

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

  Map of data types to publication element wrapper types.

8.12 relaxng.py File Reference

Namespaces

- namespace 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.

8.13 resource_set.py File Reference

Namespaces

- namespace rpki.resource_set

Classes

- class rpki.resource_set.resource_bag
- class rpki.resource_set.resource_range
- class rpki.resource_set.resource_range_as
- class rpki.resource_set.resource_range_ip
- class rpki.resource_set.resource_range_ipv4
- class rpki.resource_set.resource_range_ipv6
- class rpki.resource_set.resource_set
- class rpki.resource_set.resource_set_as
- class rpki.resource_set.resource_set_ip
- class rpki.resource_set.resource_set_ipv4
- class rpki.resource_set.resource_set_ipv6
- class rpki.resource_set.roa_prefix
- class rpki.resource_set.roa_prefix_ipv4
- class rpki.resource_set.roa_prefix_ipv6
- class rpki.resource_set.roa_prefix_set
- class rpki.resource_set.roa_prefix_set_ipv4
- class rpki.resource_set.roa_prefix_set_ipv6

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.

8.14 roa.py File Reference

Namespaces

- namespace rpki.roa

Classes

- class rpki.roa.ROAIPAddress
- class rpki.roa.ROAIPAddresses
- class rpki.roa.ROAIPAddressFamilies
- class rpki.roa.ROAIPAddressFamily
- class rpki.roa.RouteOriginAttestation

8.15 rpki_engine.py File Reference

Namespaces

- namespace rpki.rpki_engine

Classes

- class rpki.rpki_engine.ca_detail_obj
- class rpki.rpki_engine.ca_obj
- class rpki.rpki_engine.child_cert_obj
- class rpki.rpki_engine.revoked_cert_obj
- class rpki.rpki_engine.rpkid_context

8.16 rpkid.py File Reference

Namespaces

- namespace rpkid

Functions

- def rpkid.main

Variables

- string rpkid.cfg_file = "rpkid.conf"
- rpkid.profile = None

8.17 sql.py File Reference

Namespaces

- namespace rpki.sql

Classes

- class rpki.sql.session
- class rpki.sql.sql_persistant
- class rpki.sql.template

8.18 sundial.py File Reference

Namespaces

- namespace rpki.sundial

Classes

- class rpki.sundial.datetime
- class rpki.sundial.timedelta

Functions

- def rpki::sundial.now
- def rpki::sundial.test

8.19 up_down.py File Reference

Namespaces

- namespace rpki.up_down

Classes

- class rpki.up_down.base_elt
- class rpki.up_down.certificate_elt
- class rpki.up_down.class_elt
- class rpki.up_down.class_response_syntax
- class rpki.up_down.cms_msg

- class rpki.up_down.error_response_pdu
- class rpki.up_down.issue_pdu
- class rpki.up_down.issue_response_pdu
- class rpki.up_down.list_pdu
- class rpki.up_down.list_response_pdu
- class rpki.up_down.message_pdu
- class rpki.up_down.multi_uri
- class rpki.up_down.revoke_pdu
- class rpki.up_down.revoke_response_pdu
- class rpki.up_down.revoke_syntax
- class rpki.up_down.sax_handler

Variables

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

8.20 x509.py File Reference

Namespaces

- namespace rpki.x509

Classes

- class rpki.x509.CMS_object
- class rpki.x509.CRL
- class rpki.x509.DER_CMS_object
- class rpki.x509.DER_object
- class rpki.x509.PEM_converter
- class rpki.x509.PKCS10
- class rpki.x509.ROA
- class rpki.x509.RSA
- class rpki.x509.RSApublic
- class rpki.x509.SignedManifest
- class rpki.x509.X509
- class rpki.x509.XML_CMS_object

Functions

- def rpki::x509.calculate_SKI
- def rpki::x509.POWify_OID

8.21 xml_utils.py File Reference

Namespaces

- namespace rpki.xml_utils

Classes

- class rpki.xml_utils.base_elt
- class rpki.xml_utils.data_elt
- class rpki.xml_utils.msg
- class rpki.xml_utils.sax_handler

Index

__add__
rpki::sundial::datetime, 278
__call__
rpki::https::Checker, 99
rpki::log::logger, 160
__cmp__
rpki::resource_set::resource_range, 202
rpki::resource_set::roa_prefix, 227
rpki::x509::DER_object, 336
__eq__
rpki::resource_set::resource_bag, 198
__init__
pubd::pubd_context, 58
rpki::config::parser, 62
rpki::https::Checker, 99
rpki::https::httpsClient, 101
rpki::log::logger, 160
rpki::manifest::FileAndHash, 161
rpki::manifest::FilesAndHashes, 162
rpki::manifest::Manifest, 163
rpki::resource_set::resource_bag, 198
rpki::resource_set::resource_range, 202
rpki::resource_set::resource_set, 212
rpki::resource_set::roa_prefix, 227
rpki::resource_set::roa_prefix_set, 232
rpki::roa::ROAIPAddress, 236
rpki::roa::ROAIPAddresses, 237
rpki::roa::ROAIPAddressFamilies, 238
rpki::roa::ROAIPAddressFamily, 239
rpki::roa::RouteOriginAttestation, 240
rpki::rpki_engine::child_cert_obj, 256
rpki::rpki_engine::revoked_cert_obj, 260
rpki::rpki_engine::rpkid_context, 263
rpki::sql::session, 267
rpki::sql::template, 276
rpki::up_down::class_elt, 290
rpki::up_down::class_response_syntax, 294
rpki::up_down::error_response_pdu, 298
rpki::up_down::multi_uri, 311
rpki::x509::DER_object, 336
rpki::x509::PEM_converter, 341
rpki::xml_utils::sax_handler, 380
__init__.py(1871), 386
__ne__
rpki::resource_set::resource_bag, 199
__new__
rpki::ipaddrs::v4addr, 105
rpki::ipaddrs::v6addr, 107
__str__
rpki::ipaddrs::v4addr, 105
rpki::ipaddrs::v6addr, 107
rpki::resource_set::resource_bag, 199
rpki::resource_set::resource_range_as, 204
rpki::resource_set::resource_range_ip, 206
rpki::resource_set::resource_set, 212
rpki::resource_set::roa_prefix, 227
rpki::resource_set::roa_prefix_set, 232
rpki::sundial::datetime, 278
rpki::up_down::message_pdu, 308
rpki::up_down::multi_uri, 311
rpki::xml_utils::base_elt, 370
rpki::xml_utils::msg, 377
__sub__
rpki::sundial::datetime, 278
_bs2long
rpki::resource_set, 44

_comm
rpki::resource_set::resource_set, 213
_exceptions_enabled
rpki::sql::session, 269
_long2bs
rpki::resource_set, 45
_prefixlen
rpki::resource_set::resource_range_-ip, 206
_rsplit
rpki::resource_set, 45
_wrap_execute
rpki::sql::session, 267

activate
rpki::rpki_engine::ca_detail_obj, 244
address
rpki::resource_set::roa_prefix, 228
rpki::roa::ROAIPAddress, 237
addresses
rpki::roa::ROAIPAddressFamily, 239
addressFamily
rpki::roa::ROAIPAddressFamily, 239
afi
rpki::resource_set::resource_set_-ipv4, 223
rpki::resource_set::resource_set_-ipv6, 225
as_number
rpki::left_right::route_origin_elt, 149
asID
rpki::roa::RouteOriginAttestation, 241
asn
rpki::left_right::list_resources_elt, 127
rpki::resource_set::resource_bag, 200
assert_pristine
rpki::sql::session, 267
attributes
rpki::left_right::bsc_elt, 111
rpki::left_right::child_elt, 116
rpki::left_right::list_resources_elt, 127
rpki::left_right::parent_elt, 134
rpki::left_right::report_error_elt, 137
rpki::left_right::repository_elt, 142
rpki::left_right::route_origin_elt, 149
rpki::left_right::self_elt, 158
rpki::publication::client_elt, 170
rpki::publication::config_elt, 177
rpki::publication::publication_-object_elt, 191
rpki::publication::report_error_elt, 193
rpki::xml_utils::base_elt, 371

b
rpki::x509::PEM_converter, 342
base_uri
rpki::publication::client_elt, 170
BaseHTTPServer::BaseHTTPRequestHandler, 53
BaseHTTPServer::HTTPServer, 54
bits
rpki::ipaddrs::v4addr, 106
rpki::ipaddrs::v6addr, 107
booleans
rpki::left_right::bsc_elt, 111
rpki::left_right::child_elt, 116
rpki::left_right::parent_elt, 134
rpki::left_right::route_origin_elt, 149
rpki::left_right::self_elt, 158
rpki::xml_utils::base_elt, 372
bpki_cert
rpki::left_right::child_elt, 117
rpki::left_right::self_elt, 158
rpki::publication::client_elt, 170
bpki_cms_cert
rpki::left_right::parent_elt, 134
rpki::left_right::repository_elt, 142
bpki_cms_glue
rpki::left_right::parent_elt, 134
rpki::left_right::repository_elt, 143
bpki_glue

rpki::left_right::child_elt, 117
rpki::left_right::self_elt, 158
rpki::publication::client_elt, 170
bpki_https_cert
rpki::left_right::parent_elt, 134
rpki::left_right::repository_elt, 143
bpki_https_glue
rpki::left_right::parent_elt, 134
rpki::left_right::repository_elt, 143
bpki_ta
pubd::pubd_context, 59
rpki::rpki_engine::rpkid_context, 264
bsc
rpki::left_right::data_elt, 121
bscs
rpki::left_right::self_elt, 156
build
rpki::x509::ROA, 348
rpki::x509::SignedManifest, 357
build_https_ta_cache
pubd::pubd_context, 58
rpki::https, 34
rpki::rpki_engine::rpkid_context, 263

ca
rpki::rpki_engine::ca_detail_obj, 244
ca_cert_uri
rpki::rpki_engine::ca_detail_obj, 247
ca_detail
rpki::left_right::route_origin_elt, 147
rpki::rpki_engine::child_cert_obj, 256
rpki::rpki_engine::revoked_cert_obj, 260
ca_detail_id
rpki::left_right::route_origin_elt, 149
rpki::rpki_engine::child_cert_obj, 257
rpki::rpki_engine::revoked_cert_obj, 261
ca_details
rpki::rpki_engine::ca_obj, 250
ca_from_class_name
rpki::left_right::child_elt, 115
ca_id
rpki::rpki_engine::ca_detail_obj, 247
cache
rpki::sql::session, 269
cache_clear
rpki::sql::session, 268
calculate_SKI
rpki::x509, 51
call_pubd
rpki::left_right::repository_elt, 141
cas
rpki::left_right::parent_elt, 132
cert
rpki::left_right::route_origin_elt, 149
rpki::rpki_engine::child_cert_obj, 257
rpki::up_down::certificate_elt, 287
cert_url
rpki::up_down::certificate_elt, 287
rpki::up_down::class_elt, 291
certs
rpki::up_down::class_elt, 291
cfg_file
pubd, 30
rpkid, 53
characters
rpki::xml_utils::sax_handler, 380
check_allowed_uri
rpki::publication::client_elt, 169
check_for_updates
rpki::rpki_engine::ca_obj, 250
check_response
rpki::up_down::base_elt, 283
rpki::up_down::error_response_pdu, 298
rpki::up_down::issue_response_pdu, 304
check_valid_rpki
rpki::x509::PKCS10, 344
checker

rpki::https::httpsClient, 101
child
rpki::rpki_engine::child_cert_obj, 256
child_certs
rpki::left_right::child_elt, 115
rpki::rpki_engine::ca_detail_obj, 244
child_id
rpki::rpki_engine::child_cert_obj, 258
children
rpki::left_right::bsc_elt, 110
rpki::left_right::self_elt, 156
class_name
rpki::up_down::class_elt, 291
rpki::up_down::issue_pdu, 302
rpki::up_down::revoke_pdu, 314
rpki::up_down::revoke_syntax, 318
classes
rpki::up_down::class_response_-syntax, 294
clear
rpki::x509::DER_object, 336
clear_https_ta_cache
pubd::pubd_context, 58
rpki::left_right::child_elt, 117
rpki::publication::client_elt, 170
rpki::rpki_engine::rpkid_context, 263
client
rpki::https, 34
client_handler
pubd::pubd_context, 58
client_poll
rpki::left_right::self_elt, 156
close
rpki::sql::session, 268
codes
rpki::up_down::error_response_pdu, 299
columns
rpki::sql::template, 276
config.py(1873), 386
config_id
rpki::publication::config_elt, 177
ConfigParser::RawConfigParser, 54
connect
rpki::sql::session, 268
construct_sia_uri
rpki::rpki_engine::ca_obj, 251
contains
rpki::resource_set::resource_set, 213
content
rpki::x509::CMS_object, 326
rpki::x509::DER_CMS_object, 333
rpki::x509::XML_CMS_object, 367
content_class
rpki::x509::ROA, 348
rpki::x509::SignedManifest, 357
control_handler
pubd::pubd_context, 58
convert_to_seconds
rpki::sundial::timedelta, 282
create
rpki::rpki_engine::ca_detail_obj, 244
rpki::rpki_engine::ca_obj, 251
rpki::x509::PKCS10, 344
create_ca
rpki::x509::PKCS10, 344
create_top_level
rpki::xml_utils::sax_handler, 380
crl_interval
rpki::left_right::self_elt, 158
crl_uri
rpki::rpki_engine::ca_detail_obj, 244
cronjob_handler
rpki::rpki_engine::rpkid_context, 263
cur
rpki::sql::session, 269

database
rpki::sql::session, 269
datum_type
rpki::resource_set::resource_range_-as, 204
rpki::resource_set::resource_range_-ipv4, 208

rpki::resource_set::resource_range_-ipv6, 210
db
rpki::sql::session, 269
debug
rpki::log, 38
debug_cms_certs
rpki::x509::CMS_object, 326
debug_tls_certs
rpki::https, 35
decode
rpki::x509::DER_CMS_object, 333
rpki::x509::XML_CMS_object, 366
default_section
rpki::config::parser, 62
delete
rpki::rpki_engine::ca_detail_obj, 244
rpki::rpki_engine::ca_obj, 251
rpki::sql::template, 276
DER
rpki::x509::CMS_object, 326
rpki::x509::CRL, 330
rpki::x509::DER_object, 339
rpki::x509::PKCS10, 345
rpki::x509::RSA, 352
rpki::x509::RSApublic, 355
rpki::x509::X509, 362
description
rpki::up_down::error_response_pdu, 299
difference
rpki::resource_set::resource_set, 213
dirty
rpki::sql::session, 269
disable_tls_certificate_validation_-exceptions
rpki::https, 35
do_POST
rpki::https::requestHandler, 104
dump_inbound_cms
rpki::x509::XML_CMS_object, 367
dump_on_verify_failure
rpki::x509::CMS_object, 326
dump_outbound_cms
rpki::x509::XML_CMS_object, 368
dump_to_disk
rpki::x509::XML_CMS_object, 366
dumpasn1
rpki::x509::DER_object, 336
dynamic_https_trust_anchor
rpki::https::Checker, 100

e
rpki::x509::PEM_converter, 342
earlier
rpki::sundial::datetime, 278
econtent_oid
rpki::x509::CMS_object, 326
rpki::x509::ROA, 348
rpki::x509::SignedManifest, 357
rpki::x509::XML_CMS_object, 368
ee_uri
rpki::left_right::route_origin_elt, 147
ee_uri_tail
rpki::left_right::route_origin_elt, 147
element_name
rpki::left_right::bsc_elt, 111
rpki::left_right::child_elt, 117
rpki::left_right::list_resources_elt, 127
rpki::left_right::parent_elt, 134
rpki::left_right::report_error_elt, 137
rpki::left_right::repository_elt, 143
rpki::left_right::route_origin_elt, 149
rpki::left_right::self_elt, 158
rpki::publication::certificate_elt, 166
rpki::publication::client_elt, 171
rpki::publication::config_elt, 177
rpki::publication::crl_elt, 183
rpki::publication::manifest_elt, 185
rpki::publication::report_error_elt, 193
rpki::publication::roa_elt, 195
elements
rpki::left_right::bsc_elt, 111
rpki::left_right::child_elt, 117
rpki::left_right::parent_elt, 134
rpki::left_right::repository_elt, 143

rpki::left_right::self_elt, 159
rpki::publication::client_elt, 171
rpki::publication::config_elt, 177
rpki::xml_utils::base_elt, 372
empty
rpki::resource_set::resource_bag, 199
rpki::x509::DER_object, 336
enable_trace
rpki::log, 38
encode
rpki::x509::DER_CMS_object, 333
rpki::x509::XML_CMS_object, 366
encoding
rpki::left_right::cms_msg, 119
rpki::publication::cms_msg, 173
rpki::up_down::cms_msg, 296
endElement
rpki::left_right::child_elt, 116
rpki::publication::client_elt, 169
rpki::publication::publication_-object_elt, 190
rpki::up_down::base_elt, 284
rpki::up_down::certificate_elt, 287
rpki::up_down::class_elt, 290
rpki::up_down::error_response_pdu, 298
rpki::up_down::issue_pdu, 301
rpki::xml_utils::base_elt, 370
rpki::xml_utils::data_elt, 374
rpki::xml_utils::msg, 378
rpki::xml_utils::sax_handler, 380
endElementNS
rpki::xml_utils::sax_handler, 381
enforce_strict_up_down_xml_sender
rpki::left_right, 37
error
rpki::log, 39
error_code
rpki::left_right::report_error_elt, 137
rpki::publication::report_error_elt, 193
Exception, 55
exceptions
rpki::up_down::error_response_pdu, 299
exceptions.py(1873), 386
execute
rpki::sql::session, 268
executemany
rpki::sql::session, 268
expires
rpki::rpki_engine::revoked_cert_obj, 261
explicitVersion
rpki::manifest::Manifest, 164
rpki::roa::RouteOriginAttestation, 241

fetch
rpki::publication::config_elt, 176
rpki::rpki_engine::child_cert_obj, 256
fetch_active
rpki::rpki_engine::ca_obj, 251
fetch_deprecated
rpki::rpki_engine::ca_obj, 251
fetch_pending
rpki::rpki_engine::ca_obj, 252
fetch_revoked
rpki::rpki_engine::ca_obj, 252
fetchall
rpki::sql::session, 268
file
rpki::manifest::FileAndHash, 162
fileHashAlg
rpki::manifest::Manifest, 164
fileList
rpki::manifest::Manifest, 164
formats
rpki::x509::CMS_object, 327
rpki::x509::CRL, 330
rpki::x509::DER_object, 339
rpki::x509::PKCS10, 345
rpki::x509::RSA, 352
rpki::x509::RSApublic, 355
rpki::x509::X509, 362
from_exception
rpki::left_right::report_error_elt, 137
rpki::publication::report_error_elt, 193
from_resource_bag

rpki::up_down::class_elt, 290
from_rfc3779_tuples
rpki::resource_set::resource_bag, 199
from_sql
rpki::resource_set::resource_set, 213
rpki::resource_set::roa_prefix_set, 232
rpki::sundial::datetime, 279
rpki::x509::DER_object, 336
fromASN1tuple
rpki::sundial::datetime, 279
fromdatetime
rpki::sundial::datetime, 279
fromGeneralizedTime
rpki::sundial::datetime, 279
fromUTCTime
rpki::sundial::datetime, 279
fromXMLtime
rpki::sundial::datetime, 279

gAKI
rpki::x509::DER_object, 337
gctx
rpki::rpki_engine::ca_detail_obj, 247
rpki::rpki_engine::ca_obj, 253
rpki::rpki_engine::child_cert_obj, 258
rpki::rpki_engine::revoked_cert_obj, 261
rpki::sql::sql_persistant, 274
generate
rpki::x509::CRL, 329
rpki::x509::RSA, 350
generate_crl
rpki::rpki_engine::ca_detail_obj, 244
generate_manifest
rpki::rpki_engine::ca_detail_obj, 245
generate_manifest_cert
rpki::rpki_engine::ca_detail_obj, 245
generate_roa
rpki::left_right::route_origin_elt, 147
get
rpki::config::parser, 62
get_3779resources
rpki::x509::DER_object, 337
get_AIA
rpki::x509::DER_object, 337
get_AKI
rpki::x509::DER_object, 337
get_Base64
rpki::x509::DER_object, 337
get_basicConstraints
rpki::x509::DER_object, 337
get_content
rpki::x509::CMS_object, 325
get_DER
rpki::x509::CMS_object, 325
rpki::x509::CRL, 329
rpki::x509::DER_object, 337
rpki::x509::PKCS10, 345
rpki::x509::RSA, 350
rpki::x509::RSApublic, 354
rpki::x509::X509, 360
get_PEM
rpki::x509::DER_object, 338
get_POW
rpki::x509::CMS_object, 325
rpki::x509::CRL, 329
rpki::x509::RSA, 351
rpki::x509::RSApublic, 354
rpki::x509::X509, 361
get_POWpkix
rpki::x509::CRL, 330
rpki::x509::PKCS10, 345
rpki::x509::X509, 361
get_public_DER
rpki::x509::RSA, 351
get_RSApublic
rpki::x509::RSA, 351
get_SIA
rpki::x509::DER_object, 338
get_SKI
rpki::up_down::revoke_pdu, 314
rpki::x509::DER_object, 338
rpki::x509::RSA, 351

rpki::x509::RSApublic, 354
get_tlslite
rpki::x509::RSA, 351
rpki::x509::X509, 361
getIssuer
rpki::x509::CRL, 330
rpki::x509::X509, 361
getNextUpdate
rpki::x509::CRL, 330
rpki::x509::SignedManifest, 357
getNotAfter
rpki::x509::X509, 361
getNotBefore
rpki::x509::X509, 361
getPublicKey
rpki::x509::PKCS10, 345
rpki::x509::X509, 361
getSerial
rpki::x509::X509, 362
getSubject
rpki::x509::X509, 362
getThisUpdate
rpki::x509::CRL, 330
rpki::x509::SignedManifest, 357
gSKI
rpki::x509::DER_object, 338

hAKI
rpki::x509::DER_object, 338
handler_common
pubd::pubd_context, 58
handshake
rpki::https::httpsServer, 102
hash
rpki::manifest::FileAndHash, 162
hSKI
rpki::x509::DER_object, 338
https.py(1873), 387
https_server_host
pubd::pubd_context, 59
rpki::rpki_engine::rpkid_context, 264
https_server_port
pubd::pubd_context, 59
rpki::rpki_engine::rpkid_context, 264
https_ta_cache
pubd::pubd_context, 59
rpki::rpki_engine::rpkid_context, 264

index
rpki::sql::template, 276
info
rpki::log, 39
inherit
rpki::resource_set::resource_set, 214
rpki::resource_set::resource_set_as, 217
rpki::resource_set::resource_set_ip, 221
inherit_token
rpki::resource_set, 45
init
rpki::log, 38
insert
rpki::sql::template, 276
intersection
rpki::resource_set::resource_bag, 199
rpki::resource_set::resource_set, 213
ipAddrBlocks
rpki::roa::RouteOriginAttestation, 241
ipaddrs.py(1873), 388
ipv4
rpki::left_right::list_resources_elt, 127
rpki::left_right::route_origin_elt, 150
ipv6
rpki::left_right::list_resources_elt, 127
rpki::left_right::route_origin_elt, 150
irbe_cert
pubd::pubd_context, 59
rpki::rpki_engine::rpkid_context, 265
irdb_cert
rpki::rpki_engine::rpkid_context, 265

irdb_query
rpki::rpki_engine::rpkid_context, 263
irdb_url
rpki::rpki_engine::rpkid_context, 265
is_CA
rpki::x509::DER_object, 339
issubset
rpki::resource_set::resource_set, 214
issue
rpki::rpki_engine::ca_detail_obj, 245
rpki::x509::X509, 362
issue_ee
rpki::rpki_engine::ca_detail_obj, 245
issuer
rpki::up_down::class_elt, 291
issuperset
rpki::resource_set::resource_set, 214

last_crl_sn
rpki::rpki_engine::ca_obj, 253
last_issued_sn
rpki::rpki_engine::ca_obj, 253
last_manifest_sn
rpki::rpki_engine::ca_obj, 253
lastrowid
rpki::sql::session, 268
later
rpki::sundial::datetime, 279
latest_ca_cert
rpki::rpki_engine::ca_detail_obj, 247
latest_crl
rpki::rpki_engine::ca_detail_obj, 247
latest_manifest
rpki::rpki_engine::ca_detail_obj, 247
latest_manifest_cert
rpki::rpki_engine::ca_detail_obj, 247
left_right
rpki::relaxng, 43
left_right.py(1873), 388
left_right_handler
rpki::rpki_engine::rpkid_context, 264
list, 55
log.py(1873), 389
log_message
rpki::https::requestHandler, 104
long, 56
looks_like_PEM
rpki::x509::PEM_converter, 341

main
pubd, 30
rpkid, 52
make_b64elt
rpki::up_down::base_elt, 284
rpki::xml_utils::base_elt, 370
make_elt
rpki::up_down::base_elt, 284
rpki::xml_utils::base_elt, 370
make_pdu
rpki::xml_utils::base_elt, 371
make_prefix
rpki::resource_set::resource_range_-ip, 206
make_query
rpki::up_down::message_pdu, 308
make_reply
rpki::xml_utils::data_elt, 374
make_reply_clone_hook
rpki::left_right::data_elt, 121
rpki::xml_utils::data_elt, 374
manifest.py(1873), 389
manifest_private_key_id
rpki::rpki_engine::ca_detail_obj, 247
manifest_public_key
rpki::rpki_engine::ca_detail_obj, 247
manifest_uri
rpki::rpki_engine::ca_detail_obj, 245
manifestNumber
rpki::manifest::Manifest, 164
map

rpki::sql::template, 276
max
rpki::resource_set::resource_range, 202
rpki::resource_set::roa_prefix, 227
max_prefixlen
rpki::resource_set::roa_prefix, 228
maxLength
rpki::roa::ROAIPAddress, 237
min
rpki::resource_set::resource_range, 202
rpki::resource_set::resource_range_-as, 204
rpki::resource_set::roa_prefix, 227
multiget
rpki::config::parser, 62

name
rpki::left_right::sax_handler, 152
rpki::publication::sax_handler, 197
rpki::up_down::sax_handler, 321
name2oid
rpki::oids, 40
name2type
rpki::up_down::message_pdu, 309
next_crl_number
rpki::rpki_engine::ca_obj, 252
next_manifest_number
rpki::rpki_engine::ca_obj, 252
next_serial_number
rpki::rpki_engine::ca_obj, 252
nextUpdate
rpki::manifest::Manifest, 164
normalize_chain
rpki::x509::X509, 362
note
rpki::log, 39
now
rpki::sundial, 49
nsmap
rpki::left_right::left_right_-namespace, 124
rpki::publication::publication_-namespace, 188
rpki::up_down, 50
obj2elt
rpki::publication, 42
object, 56
object_delete
rpki::left_right::repository_elt, 141
object_write
rpki::left_right::repository_elt, 142
oid2name
rpki::oids, 40
oids.py(1873), 390
other_clear
rpki::x509::CMS_object, 327
rpki::x509::DER_object, 340
oversized
rpki::resource_set::resource_bag, 199

parent
rpki::rpki_engine::ca_obj, 252
parent_id
rpki::rpki_engine::ca_obj, 253
parent_resource_class
rpki::rpki_engine::ca_obj, 253
parents
rpki::left_right::bsc_elt, 110
rpki::left_right::child_elt, 116
rpki::left_right::repository_elt, 142
rpki::left_right::self_elt, 156
parse
rpki::sundial::timedelta, 282
parse_rfc3779_tuple
rpki::resource_set::resource_set_as, 216
rpki::resource_set::resource_set_ip, 220
parse_str
rpki::resource_set::resource_set_as, 216
rpki::resource_set::resource_set_ip, 220
rpki::resource_set::roa_prefix_set, 232
password
rpki::sql::session, 269
payload

rpki::publication::publication_-object_elt, 191
rpki::up_down::message_pdu, 309
payload_type
rpki::publication::certificate_elt, 166
rpki::publication::crl_elt, 183
rpki::publication::manifest_elt, 185
rpki::publication::roa_elt, 195
pdu
rpki::left_right::sax_handler, 152
rpki::publication::sax_handler, 197
rpki::up_down::sax_handler, 321
pdus
rpki::left_right::msg, 129
rpki::publication::msg, 186
pem_converter
rpki::x509::CRL, 331
rpki::x509::DER_object, 340
rpki::x509::PKCS10, 345
rpki::x509::ROA, 348
rpki::x509::RSA, 352
rpki::x509::RSApublic, 355
rpki::x509::SignedManifest, 358
rpki::x509::X509, 363
pem_dump_tls_certs
rpki::https::Checker, 100
ping
rpki::sql::session, 268
pkcs10
rpki::up_down::issue_pdu, 302
pkcs10_request
rpki::left_right::bsc_elt, 112
PKIX_threshhold
rpki::sundial::datetime, 281
POW
rpki::x509::CMS_object, 327
rpki::x509::CRL, 331
rpki::x509::RSA, 352
rpki::x509::RSApublic, 355
rpki::x509::X509, 363
POWify_OID
rpki::x509, 51
POWpkix
rpki::x509::CRL, 331
rpki::x509::PKCS10, 346
rpki::x509::X509, 363
prefix_type
rpki::resource_set::roa_prefix_set_-ipv4, 234
rpki::resource_set::roa_prefix_set_-ipv6, 235
prefixlen
rpki::resource_set::roa_prefix, 228
pretty_print_content
rpki::x509::XML_CMS_object, 367
print_on_der_error
rpki::x509::CMS_object, 327
priority
rpki::log::logger, 161
private_key_id
rpki::left_right::bsc_elt, 112
rpki::rpki_engine::ca_detail_obj, 247
profile
pubd, 30
rpkid, 53
pubd, 30
cfg_file, 30
main, 30
profile, 30
pubd.py(1853), 390
pubd::pubd_context, 57
__init__, 58
bpki_ta, 59
build_https_ta_cache, 58
clear_https_ta_cache, 58
client_handler, 58
control_handler, 58
handler_common, 58
https_server_host, 59
https_server_port, 59
https_ta_cache, 59
irbe_cert, 59
pubd_cert, 59
pubd_key, 59
publication_base, 59
sql, 59
pubd_cert
pubd::pubd_context, 59
pubd_key
pubd::pubd_context, 59
public_key

rpki::rpki_engine::ca_detail_obj, 247
publication
rpki::relaxng, 43
publication.py(1873), 390
publication_base
pubd::pubd_context, 59
publication_kludge_base
rpki::rpki_engine::rpkid_context, 265
publish
rpki::left_right::repository_elt, 142
pydatetime::datetime, 60
pydatetime::timedelta, 61

query
rpki::up_down::issue_pdu, 301
rpki::up_down::list_pdu, 305
rpki::up_down::revoke_pdu, 314
query_up_down
rpki::left_right::parent_elt, 132

range_type
rpki::resource_set::resource_set_as, 217
rpki::resource_set::resource_set_-ipv4, 223
rpki::resource_set::resource_set_-ipv6, 225
rpki::resource_set::roa_prefix_ipv4, 229
rpki::resource_set::roa_prefix_ipv6, 231
read_attrs
rpki::xml_utils::base_elt, 371
recipient
rpki::up_down::message_pdu, 310
refuse_tls_ca_certs
rpki::https::Checker, 100
regen_margin
rpki::left_right::self_elt, 159
regenerate_crls_and_manifests
rpki::left_right::self_elt, 156
regenerate_roa
rpki::left_right::route_origin_elt, 147
regexp
rpki::sundial::timedelta, 282
reissue
rpki::rpki_engine::child_cert_obj, 257
rekey
rpki::rpki_engine::ca_obj, 252
relaxng.py(1838), 391
repositories
rpki::left_right::bsc_elt, 111
rpki::left_right::self_elt, 156
repository
rpki::left_right::parent_elt, 133
req_resource_set_as
rpki::up_down::certificate_elt, 288
rpki::up_down::issue_pdu, 302
req_resource_set_ipv4
rpki::up_down::certificate_elt, 288
rpki::up_down::issue_pdu, 302
req_resource_set_ipv6
rpki::up_down::certificate_elt, 288
rpki::up_down::issue_pdu, 302
require_crls
rpki::x509::CMS_object, 327
resource_set.py(1873), 392
resource_set_as
rpki::up_down::class_elt, 291
resource_set_ipv4
rpki::up_down::class_elt, 292
resource_set_ipv6
rpki::up_down::class_elt, 292
resource_set_notafter
rpki::up_down::class_elt, 292
resource_set_type
rpki::resource_set::roa_prefix_set_-ipv4, 234
rpki::resource_set::roa_prefix_set_-ipv6, 235
result
rpki::xml_utils::sax_handler, 381
revoke
rpki::rpki_engine::ca_detail_obj, 245
rpki::rpki_engine::ca_obj, 253
rpki::rpki_engine::child_cert_obj, 257

rpki::rpki_engine::revoked_cert_obj, 260
revoked
rpki::rpki_engine::revoked_cert_obj, 261
revoked_certs
rpki::rpki_engine::ca_detail_obj, 246
roa
rpki::left_right::route_origin_elt, 150
roa.py(1873), 393
roa_uri
rpki::left_right::route_origin_elt, 147
route_origins
rpki::left_right::self_elt, 156
rpki::rpki_engine::ca_detail_obj, 246
rpki, 31
rpki.config, 31
rpki.exceptions, 32
rpki.https, 33
rpki.ipaddrs, 35
rpki.left_right, 36
rpki.log, 37
rpki.manifest, 39
rpki.oids, 40
rpki.publication, 41
rpki.relaxng, 42
rpki.resource_set, 43
rpki.roa, 45
rpki.rpki_engine, 47
rpki.sql, 47
rpki.sundial, 48
rpki.up_down, 49
rpki.x509, 50
rpki.xml_utils, 52
rpki::config::parser, 61
__init__, 62
default_section, 62
get, 62
multiget, 62
rpki::exceptions::BadClassNameSyntax, 63
rpki::exceptions::BadContactURL, 64
rpki::exceptions::BadIRDBReply, 65
rpki::exceptions::BadIssueResponse, 66
rpki::exceptions::BadPKCS10, 67
rpki::exceptions::BadQuery, 68
rpki::exceptions::BadSender, 69
rpki::exceptions::BadStatusCode, 70
rpki::exceptions::BadURISyntax, 71
rpki::exceptions::BSCNotFound, 72
rpki::exceptions::ChildNotFound, 73
rpki::exceptions::ClassNameMismatch, 74
rpki::exceptions::CMSCRLNotSet, 75
rpki::exceptions::CMSVerificationFailed, 76
rpki::exceptions::DBConsistancyError, 77
rpki::exceptions::DERObjectConversionError, 78
rpki::exceptions::EmptyPEM, 79
rpki::exceptions::HTTPRequestFailed, 80
rpki::exceptions::MissingCMSCRL, 81
rpki::exceptions::MissingCMSEEcert, 82
rpki::exceptions::MultipleTLSEECert, 83
rpki::exceptions::MustBePrefix, 84
rpki::exceptions::NotACertificateChain, 85
rpki::exceptions::NotFound, 86
rpki::exceptions::NotImplementedYet, 87
rpki::exceptions::NotInDatabase, 88
rpki::exceptions::ReceivedTLSCACert, 89
rpki::exceptions::RPKI_Exception, 89
rpki::exceptions::ServerShuttingDown, 90
rpki::exceptions::SKIMismatch, 91
rpki::exceptions::SubprocessError, 92
rpki::exceptions::TLSValidationError, 93
rpki::exceptions::UnexpectedCMSCerts, 94
rpki::exceptions::UnexpectedCMSCRLs, 95
rpki::exceptions::UnparsableCMSDER, 96
rpki::exceptions::UpstreamError, 97
rpki::exceptions::WrongEContentType, 98

rpki::https
build_https_ta_cache, 34
client, 34
debug_tls_certs, 35
disable_tls_certificate_validation_-exceptions, 35
rpki_content_type, 35
server, 34
tlslite_certChain, 35
rpki::https::Checker, 98
__call__, 99
__init__, 99
dynamic_https_trust_anchor, 100
pem_dump_tls_certs, 100
refuse_tls_ca_certs, 100
x509store, 100
x509store_thunk, 99
rpki::https::httpsClient, 100
__init__, 101
checker, 101
rpki::https::httpsServer, 102
handshake, 102
rpki_checker, 103
rpki_server_cert, 103
rpki_server_key, 103
rpki_sessionCache, 103
rpki::https::requestHandler, 103
do_POST, 104
log_message, 104
rpki_find_handler, 104
rpki_handlers, 104
rpki::ipaddrs::v4addr, 105
__new__, 105
__str__, 105
bits, 106
rpki::ipaddrs::v6addr, 106
__new__, 107
__str__, 107
bits, 107
rpki::left_right
enforce_strict_up_down_xml_-sender, 37
rpki::left_right::bsc_elt, 109
attributes, 111
booleans, 111
children, 110
element_name, 111
elements, 111
parents, 110
pkcs10_request, 112
private_key_id, 112
repositories, 111
serve_pre_save_hook, 111
signing_cert, 112
signing_cert_crl, 112
sql_template, 112
rpki::left_right::child_elt, 114
attributes, 116
booleans, 116
bpki_cert, 117
bpki_glue, 117
ca_from_class_name, 115
child_certs, 115
clear_https_ta_cache, 117
element_name, 117
elements, 117
endElement, 116
parents, 116
serve_post_save_hook, 116
serve_up_down, 116
sql_template, 117
rpki::left_right::cms_msg, 118
encoding, 119
saxify, 119
schema, 119
rpki::left_right::data_elt, 120
bsc, 121
make_reply_clone_hook, 121
self, 121
serve_fetch_all, 121
serve_fetch_one, 121
unimplemented_control, 122
rpki::left_right::left_right_namespace, 123
nsmap, 124
xmlns, 124
rpki::left_right::list_resources_elt, 125
asn, 127
attributes, 127
element_name, 127
ipv4, 127
ipv6, 127

startElement, 126
toXML, 126
valid_until, 127
rpki::left_right::msg, 128
pdus, 129
serve_top_level, 128
version, 129
rpki::left_right::parent_elt, 131
attributes, 134
booleans, 134
bpki_cms_cert, 134
bpki_cms_glue, 134
bpki_https_cert, 134
bpki_https_glue, 134
cas, 132
element_name, 134
elements, 134
query_up_down, 132
repository, 133
serve_post_save_hook, 133
serve_rekey, 133
serve_revoke, 133
sql_template, 135
rpki::left_right::report_error_elt, 136
attributes, 137
element_name, 137
error_code, 137
from_exception, 137
self_id, 138
rpki::left_right::repository_elt, 140
attributes, 142
bpki_cms_cert, 142
bpki_cms_glue, 143
bpki_https_cert, 143
bpki_https_glue, 143
call_pubd, 141
element_name, 143
elements, 143
object_delete, 141
object_write, 142
parents, 142
publish, 142
sql_template, 143
uri_to_filename, 142
use_pubd, 143
withdraw, 142
rpki::left_right::route_origin_elt, 145
as_number, 149
attributes, 149
booleans, 149
ca_detail, 147
ca_detail_id, 149
cert, 149
ee_uri, 147
ee_uri_tail, 147
element_name, 149
generate_roa, 147
ipv4, 150
ipv6, 150
regenerate_roa, 147
roa, 150
roa_uri, 147
serve_post_save_hook, 148
sql_delete_hook, 148
sql_fetch_hook, 148
sql_insert_hook, 148
sql_template, 150
startElement, 148
update_roa, 148
withdraw_roa, 149
rpki::left_right::sax_handler, 151
name, 152
pdu, 152
version, 152
rpki::left_right::self_elt, 154
attributes, 158
booleans, 158
bpki_cert, 158
bpki_glue, 158
bscs, 156
children, 156
client_poll, 156
crl_interval, 158
element_name, 158
elements, 159
parents, 156
regen_margin, 159
regenerate_crls_and_manifests, 156
repositories, 156
route_origins, 156
self_id, 159
serve_fetch_all, 157

serve_fetch_one, 157
serve_post_save_hook, 157
serve_rekey, 157
serve_revoke, 157
sql_template, 159
update_children, 157
update_roas, 158
use_hsm, 159
rpki::log
debug, 38
enable_trace, 38
error, 39
info, 39
init, 38
note, 39
set_trace, 38
trace, 38
warn, 39
rpki::log::logger, 160
__call__, 160
__init__, 160
priority, 161
rpki::manifest::FileAndHash, 161
__init__, 161
file, 162
hash, 162
rpki::manifest::FilesAndHashes, 162
__init__, 162
rpki::manifest::Manifest, 163
__init__, 163
explicitVersion, 164
fileHashAlg, 164
fileList, 164
manifestNumber, 164
nextUpdate, 164
thisUpdate, 164
version, 164
rpki::oids
name2oid, 40
oid2name, 40
rpki::publication
obj2elt, 42
rpki::publication::certificate_elt, 165
element_name, 166
payload_type, 166
rpki::publication::client_elt, 168
attributes, 170
base_uri, 170
bpki_cert, 170
bpki_glue, 170
check_allowed_uri, 169
clear_https_ta_cache, 170
element_name, 171
elements, 171
endElement, 169
serve_fetch_all, 169
serve_fetch_one, 170
serve_post_save_hook, 170
sql_template, 171
rpki::publication::cms_msg, 172
encoding, 173
saxify, 173
schema, 173
rpki::publication::config_elt, 175
attributes, 177
config_id, 177
element_name, 177
elements, 177
fetch, 176
serve_fetch_one, 176
serve_set, 177
sql_template, 178
startElement, 177
wired_in_config_id, 178
rpki::publication::control_elt, 180
serve_dispatch, 181
rpki::publication::crl_elt, 182
element_name, 183
payload_type, 183
rpki::publication::manifest_elt, 184
element_name, 185
payload_type, 185
rpki::publication::msg, 185
pdus, 186
serve_top_level, 186
version, 186
rpki::publication::publication_-namespace, 187
nsmap, 188
xmlns, 188
rpki::publication::publication_object_elt, 189

attributes, 191
endElement, 190
payload, 191
serve_dispatch, 190
serve_publish, 190
serve_withdraw, 190
toXML, 191
uri_to_filename, 191
rpki::publication::report_error_elt, 192
attributes, 193
element_name, 193
error_code, 193
from_exception, 193
rpki::publication::roa_elt, 194
element_name, 195
payload_type, 195
rpki::publication::sax_handler, 196
name, 197
pdu, 197
version, 197
rpki::relaxng
left_right, 43
publication, 43
up_down, 43
rpki::resource_set
_bs2long, 44
_long2bs, 45
_rsplit, 45
inherit_token, 45
test1, 45
test2, 45
rpki::resource_set::resource_bag, 197
__eq__, 198
__init__, 198
__ne__, 199
__str__, 199
asn, 200
empty, 199
from_rfc3779_tuples, 199
intersection, 199
oversized, 199
undersized, 199
union, 199
v4, 200
v6, 200
valid_until, 200
rpki::resource_set::resource_range, 201
__cmp__, 202
__init__, 202
max, 202
min, 202
rpki::resource_set::resource_range_as, 203
__str__, 204
datum_type, 204
min, 204
to_rfc3779_tuple, 204
rpki::resource_set::resource_range_ip, 205
__str__, 206
_prefixlen, 206
make_prefix, 206
to_rfc3779_tuple, 206
rpki::resource_set::resource_range_ipv4, 207
datum_type, 208
rpki::resource_set::resource_range_ipv6, 209
datum_type, 210
rpki::resource_set::resource_set, 211
__init__, 212
__str__, 212
_comm, 213
contains, 213
difference, 213
from_sql, 213
inherit, 214
intersection, 213
issubset, 214
issuperset, 214
symmetric_difference, 214
union, 214
rpki::resource_set::resource_set_as, 215
inherit, 217
parse_rfc3779_tuple, 216
parse_str, 216
range_type, 217
to_rfc3779_tuple, 216
rpki::resource_set::resource_set_ip, 219
inherit, 221
parse_rfc3779_tuple, 220
parse_str, 220

to_rfc3779_tuple, 220
rpki::resource_set::resource_set_ipv4, 222
afi, 223
range_type, 223
rpki::resource_set::resource_set_ipv6, 224
afi, 225
range_type, 225
rpki::resource_set::roa_prefix, 226
__cmp__, 227
__init__, 227
__str__, 227
address, 228
max, 227
max_prefixlen, 228
min, 227
prefixlen, 228
to_resource_range, 227
to_roa_tuple, 228
rpki::resource_set::roa_prefix_ipv4, 229
range_type, 229
rpki::resource_set::roa_prefix_ipv6, 230
range_type, 231
rpki::resource_set::roa_prefix_set, 231
__init__, 232
__str__, 232
from_sql, 232
parse_str, 232
to_resource_set, 233
to_roa_tuple, 233
rpki::resource_set::roa_prefix_set_ipv4, 233
prefix_type, 234
resource_set_type, 234
rpki::resource_set::roa_prefix_set_ipv6, 235
prefix_type, 235
resource_set_type, 235
rpki::roa::ROAIPAddress, 236
__init__, 236
address, 237
maxLength, 237
rpki::roa::ROAIPAddresses, 237
__init__, 237
rpki::roa::ROAIPAddressFamilies, 238
__init__, 238
rpki::roa::ROAIPAddressFamily, 239
__init__, 239
addresses, 239
addressFamily, 239
rpki::roa::RouteOriginAttestation, 240
__init__, 240
asID, 241
explicitVersion, 241
ipAddrBlocks, 241
version, 241
rpki::rpki_engine::ca_detail_obj, 242
activate, 244
ca, 244
ca_cert_uri, 247
ca_id, 247
child_certs, 244
create, 244
crl_uri, 244
delete, 244
gctx, 247
generate_crl, 244
generate_manifest, 245
generate_manifest_cert, 245
issue, 245
issue_ee, 245
latest_ca_cert, 247
latest_crl, 247
latest_manifest, 247
latest_manifest_cert, 247
manifest_private_key_id, 247
manifest_public_key, 247
manifest_uri, 245
private_key_id, 247
public_key, 247
revoke, 245
revoked_certs, 246
route_origins, 246
sql_decode, 246
sql_template, 248
state, 248
update, 246
rpki::rpki_engine::ca_obj, 249
ca_details, 250
check_for_updates, 250
construct_sia_uri, 251

create, 251
delete, 251
fetch_active, 251
fetch_deprecated, 251
fetch_pending, 252
fetch_revoked, 252
gctx, 253
last_crl_sn, 253
last_issued_sn, 253
last_manifest_sn, 253
next_crl_number, 252
next_manifest_number, 252
next_serial_number, 252
parent, 252
parent_id, 253
parent_resource_class, 253
rekey, 252
revoke, 253
sia_uri, 253
sql_template, 253
rpki::rpki_engine::child_cert_obj, 255
__init__, 256
ca_detail, 256
ca_detail_id, 257
cert, 257
child, 256
child_id, 258
fetch, 256
gctx, 258
reissue, 257
revoke, 257
sql_template, 258
uri, 257
uri_tail, 257
rpki::rpki_engine::revoked_cert_obj, 259
__init__, 260
ca_detail, 260
ca_detail_id, 261
expires, 261
gctx, 261
revoke, 260
revoked, 261
serial, 261
sql_template, 261
rpki::rpki_engine::rpkid_context, 262
__init__, 263
bpki_ta, 264
build_https_ta_cache, 263
clear_https_ta_cache, 263
cronjob_handler, 263
https_server_host, 264
https_server_port, 264
https_ta_cache, 264
irbe_cert, 265
irdb_cert, 265
irdb_query, 263
irdb_url, 265
left_right_handler, 264
publication_kludge_base, 265
rpkid_cert, 265
rpkid_key, 265
sql, 265
up_down_handler, 264
rpki::sql::session, 266
__init__, 267
_exceptions_enabled, 269
_wrap_execute, 267
assert_pristine, 267
cache, 269
cache_clear, 268
close, 268
connect, 268
cur, 269
database, 269
db, 269
dirty, 269
execute, 268
executemany, 268
fetchall, 268
lastrowid, 268
password, 269
ping, 268
sweep, 268
username, 269
rpki::sql::sql_persistant, 270
gctx, 274
sql_debug, 274
sql_decode, 271
sql_delete, 271
sql_delete_hook, 271
sql_deleted, 274
sql_encode, 272

sql_fetch, 272
sql_fetch_all, 272
sql_fetch_hook, 272
sql_fetch_where, 272
sql_fetch_where1, 273
sql_in_db, 274
sql_init, 273
sql_insert_hook, 273
sql_is_dirty, 273
sql_mark_clean, 273
sql_mark_deleted, 273
sql_mark_dirty, 274
sql_store, 274
sql_update_hook, 274
rpki::sql::template, 275
__init__, 276
columns, 276
delete, 276
index, 276
insert, 276
map, 276
select, 276
table, 276
update, 276
rpki::sundial
now, 49
test, 49
rpki::sundial::datetime, 277
__add__, 278
__str__, 278
__sub__, 278
earlier, 278
from_sql, 279
fromASN1tuple, 279
fromdatetime, 279
fromGeneralizedTime, 279
fromUTCTime, 279
fromXMLtime, 279
later, 279
PKIX_threshhold, 281
to_sql, 280
toASN1tuple, 280
toGeneralizedTime, 280
totimestamp, 280
toUTCTime, 280
toXMLtime, 280
rpki::sundial::timedelta, 281
convert_to_seconds, 282
parse, 282
regexp, 282
rpki::up_down
nsmap, 50
xmlns, 50
rpki::up_down::base_elt, 283
check_response, 283
endElement, 284
make_b64elt, 284
make_elt, 284
serve_pdu, 284
startElement, 284
rpki::up_down::certificate_elt, 286
cert, 287
cert_url, 287
endElement, 287
req_resource_set_as, 288
req_resource_set_ipv4, 288
req_resource_set_ipv6, 288
startElement, 287
toXML, 287
rpki::up_down::class_elt, 289
__init__, 290
cert_url, 291
certs, 291
class_name, 291
endElement, 290
from_resource_bag, 290
issuer, 291
resource_set_as, 291
resource_set_ipv4, 292
resource_set_ipv6, 292
resource_set_notafter, 292
startElement, 291
suggested_sia_head, 292
to_resource_bag, 291
toXML, 291
rpki::up_down::class_response_syntax, 293
__init__, 294
classes, 294
startElement, 294
toXML, 294
rpki::up_down::cms_msg, 295

encoding, 296
saxify, 296
schema, 296
rpki::up_down::error_response_pdu, 297
__init__, 298
check_response, 298
codes, 299
description, 299
endElement, 298
exceptions, 299
status, 299
toXML, 298
rpki::up_down::issue_pdu, 300
class_name, 302
endElement, 301
pkcs10, 302
query, 301
req_resource_set_as, 302
req_resource_set_ipv4, 302
req_resource_set_ipv6, 302
serve_pdu, 301
startElement, 301
toXML, 302
rpki::up_down::issue_response_pdu, 303
check_response, 304
rpki::up_down::list_pdu, 304
query, 305
serve_pdu, 305
toXML, 305
rpki::up_down::list_response_pdu, 306
rpki::up_down::message_pdu, 307
__str__, 308
make_query, 308
name2type, 309
payload, 309
recipient, 310
sender, 310
serve_error, 308
serve_top_level, 309
startElement, 309
toXML, 309
type, 310
type2name, 310
version, 310
rpki::up_down::multi_uri, 311
__init__, 311
__str__, 311
rsync, 311
rpki::up_down::revoke_pdu, 313
class_name, 314
get_SKI, 314
query, 314
serve_pdu, 314
ski, 314
rpki::up_down::revoke_response_pdu, 316
rpki::up_down::revoke_syntax, 317
class_name, 318
ski, 318
startElement, 318
toXML, 318
rpki::up_down::sax_handler, 320
name, 321
pdu, 321
version, 321
rpki::x509
calculate_SKI, 51
POWify_OID, 51
rpki::x509::CMS_object, 323
content, 326
debug_cms_certs, 326
DER, 326
dump_on_verify_failure, 326
econtent_oid, 326
formats, 327
get_content, 325
get_DER, 325
get_POW, 325
other_clear, 327
POW, 327
print_on_der_error, 327
require_crls, 327
set_content, 325
sign, 325
verify, 326
rpki::x509::CRL, 328
DER, 330
formats, 330
generate, 329
get_DER, 329
get_POW, 329
get_POWpkix, 330

getIssuer, 330
getNextUpdate, 330
getThisUpdate, 330
pem_converter, 331
POW, 331
POWpkix, 331
rpki::x509::DER_CMS_object, 332
content, 333
decode, 333
encode, 333
rpki::x509::DER_object, 334
__cmp__, 336
__init__, 336
clear, 336
DER, 339
dumpasn1, 336
empty, 336
formats, 339
from_sql, 336
gAKI, 337
get_3779resources, 337
get_AIA, 337
get_AKI, 337
get_Base64, 337
get_basicConstraints, 337
get_DER, 337
get_PEM, 338
get_SIA, 338
get_SKI, 338
gSKI, 338
hAKI, 338
hSKI, 338
is_CA, 339
other_clear, 340
pem_converter, 340
set, 339
to_sql, 339
rpki::x509::PEM_converter, 340
__init__, 341
b, 342
e, 342
looks_like_PEM, 341
to_DER, 341
to_PEM, 341
rpki::x509::PKCS10, 343
check_valid_rpki, 344
create, 344
create_ca, 344
DER, 345
formats, 345
get_DER, 345
get_POWpkix, 345
getPublicKey, 345
pem_converter, 345
POWpkix, 346
rpki::x509::ROA, 347
build, 348
content_class, 348
econtent_oid, 348
pem_converter, 348
rpki::x509::RSA, 349
DER, 352
formats, 352
generate, 350
get_DER, 350
get_POW, 351
get_public_DER, 351
get_RSApublic, 351
get_SKI, 351
get_tlslite, 351
pem_converter, 352
POW, 352
tlslite, 352
rpki::x509::RSApublic, 353
DER, 355
formats, 355
get_DER, 354
get_POW, 354
get_SKI, 354
pem_converter, 355
POW, 355
rpki::x509::SignedManifest, 356
build, 357
content_class, 357
econtent_oid, 357
getNextUpdate, 357
getThisUpdate, 357
pem_converter, 358
rpki::x509::X509, 359
DER, 362
formats, 362
get_DER, 360

get_POW, 361
get_POWpkix, 361
get_tlslite, 361
getIssuer, 361
getNotAfter, 361
getNotBefore, 361
getPublicKey, 361
getSerial, 362
getSubject, 362
issue, 362
normalize_chain, 362
pem_converter, 363
POW, 363
POWpkix, 363
tlslite, 363
rpki::x509::XML_CMS_object, 365
content, 367
decode, 366
dump_inbound_cms, 367
dump_outbound_cms, 368
dump_to_disk, 366
econtent_oid, 368
encode, 366
pretty_print_content, 367
schema_check, 367
unwrap, 367
wrap, 367
rpki::xml_utils::base_elt, 369
__str__, 370
attributes, 371
booleans, 372
elements, 372
endElement, 370
make_b64elt, 370
make_elt, 370
make_pdu, 371
read_attrs, 371
startElement, 371
toXML, 371
rpki::xml_utils::data_elt, 373
endElement, 374
make_reply, 374
make_reply_clone_hook, 374
serve_create, 374
serve_destroy, 374
serve_dispatch, 375
serve_get, 375
serve_list, 375
serve_post_save_hook, 375
serve_pre_save_hook, 375
serve_set, 375
toXML, 376
unimplemented_control, 376
rpki::xml_utils::msg, 377
__str__, 377
endElement, 378
startElement, 378
toXML, 378
type, 378
version, 378
rpki::xml_utils::sax_handler, 379
__init__, 380
characters, 380
create_top_level, 380
endElement, 380
endElementNS, 381
result, 381
saxify, 381
stack, 381
startElement, 381
startElementNS, 381
text, 382
rpki_checker
rpki::https::httpsServer, 103
rpki_content_type
rpki::https, 35
rpki_engine.py(1873), 393
rpki_find_handler
rpki::https::requestHandler, 104
rpki_handlers
rpki::https::requestHandler, 104
rpki_server_cert
rpki::https::httpsServer, 103
rpki_server_key
rpki::https::httpsServer, 103
rpki_sessionCache
rpki::https::httpsServer, 103
rpkid, 52
cfg_file, 53
main, 52
profile, 53
rpkid.py(1848), 393

rpkid_cert
rpki::rpki_engine::rpkid_context, 265
rpkid_key
rpki::rpki_engine::rpkid_context, 265
rsync
rpki::up_down::multi_uri, 311

saxify
rpki::left_right::cms_msg, 119
rpki::publication::cms_msg, 173
rpki::up_down::cms_msg, 296
rpki::xml_utils::sax_handler, 381
schema
rpki::left_right::cms_msg, 119
rpki::publication::cms_msg, 173
rpki::up_down::cms_msg, 296
schema_check
rpki::x509::XML_CMS_object, 367
select
rpki::sql::template, 276
self
rpki::left_right::data_elt, 121
self_id
rpki::left_right::report_error_elt, 138
rpki::left_right::self_elt, 159
sender
rpki::up_down::message_pdu, 310
Sequence, 382
SequenceOf, 383
serial
rpki::rpki_engine::revoked_cert_obj, 261
serve_create
rpki::xml_utils::data_elt, 374
serve_destroy
rpki::xml_utils::data_elt, 374
serve_dispatch
rpki::publication::control_elt, 181
rpki::publication::publication_-object_elt, 190
rpki::xml_utils::data_elt, 375
serve_error
rpki::up_down::message_pdu, 308
serve_fetch_all
rpki::left_right::data_elt, 121
rpki::left_right::self_elt, 157
rpki::publication::client_elt, 169
serve_fetch_one
rpki::left_right::data_elt, 121
rpki::left_right::self_elt, 157
rpki::publication::client_elt, 170
rpki::publication::config_elt, 176
serve_get
rpki::xml_utils::data_elt, 375
serve_list
rpki::xml_utils::data_elt, 375
serve_pdu
rpki::up_down::base_elt, 284
rpki::up_down::issue_pdu, 301
rpki::up_down::list_pdu, 305
rpki::up_down::revoke_pdu, 314
serve_post_save_hook
rpki::left_right::child_elt, 116
rpki::left_right::parent_elt, 133
rpki::left_right::route_origin_elt, 148
rpki::left_right::self_elt, 157
rpki::publication::client_elt, 170
rpki::xml_utils::data_elt, 375
serve_pre_save_hook
rpki::left_right::bsc_elt, 111
rpki::xml_utils::data_elt, 375
serve_publish
rpki::publication::publication_-object_elt, 190
serve_rekey
rpki::left_right::parent_elt, 133
rpki::left_right::self_elt, 157
serve_revoke
rpki::left_right::parent_elt, 133
rpki::left_right::self_elt, 157
serve_set
rpki::publication::config_elt, 177
rpki::xml_utils::data_elt, 375
serve_top_level
rpki::left_right::msg, 128
rpki::publication::msg, 186
rpki::up_down::message_pdu, 309
serve_up_down
rpki::left_right::child_elt, 116

serve_withdraw
rpki::publication::publication_-object_elt, 190
server
rpki::https, 34
set
rpki::x509::DER_object, 339
set_content
rpki::x509::CMS_object, 325
set_trace
rpki::log, 38
sia_uri
rpki::rpki_engine::ca_obj, 253
sign
rpki::x509::CMS_object, 325
signing_cert
rpki::left_right::bsc_elt, 112
signing_cert_crl
rpki::left_right::bsc_elt, 112
ski
rpki::up_down::revoke_pdu, 314
rpki::up_down::revoke_syntax, 318
sql
pubd::pubd_context, 59
rpki::rpki_engine::rpkid_context, 265
sql.py(1873), 394
sql_debug
rpki::sql::sql_persistant, 274
sql_decode
rpki::rpki_engine::ca_detail_obj, 246
rpki::sql::sql_persistant, 271
sql_delete
rpki::sql::sql_persistant, 271
sql_delete_hook
rpki::left_right::route_origin_elt, 148
rpki::sql::sql_persistant, 271
sql_deleted
rpki::sql::sql_persistant, 274
sql_encode
rpki::sql::sql_persistant, 272
sql_fetch
rpki::sql::sql_persistant, 272
sql_fetch_all
rpki::sql::sql_persistant, 272
sql_fetch_hook
rpki::left_right::route_origin_elt, 148
rpki::sql::sql_persistant, 272
sql_fetch_where
rpki::sql::sql_persistant, 272
sql_fetch_where1
rpki::sql::sql_persistant, 273
sql_in_db
rpki::sql::sql_persistant, 274
sql_init
rpki::sql::sql_persistant, 273
sql_insert_hook
rpki::left_right::route_origin_elt, 148
rpki::sql::sql_persistant, 273
sql_is_dirty
rpki::sql::sql_persistant, 273
sql_mark_clean
rpki::sql::sql_persistant, 273
sql_mark_deleted
rpki::sql::sql_persistant, 273
sql_mark_dirty
rpki::sql::sql_persistant, 274
sql_store
rpki::sql::sql_persistant, 274
sql_template
rpki::left_right::bsc_elt, 112
rpki::left_right::child_elt, 117
rpki::left_right::parent_elt, 135
rpki::left_right::repository_elt, 143
rpki::left_right::route_origin_elt, 150
rpki::left_right::self_elt, 159
rpki::publication::client_elt, 171
rpki::publication::config_elt, 178
rpki::rpki_engine::ca_detail_obj, 248
rpki::rpki_engine::ca_obj, 253
rpki::rpki_engine::child_cert_obj, 258
rpki::rpki_engine::revoked_cert_obj, 261
sql_update_hook
rpki::sql::sql_persistant, 274

stack
rpki::xml_utils::sax_handler, 381
startElement
rpki::left_right::list_resources_elt, 126
rpki::left_right::route_origin_elt, 148
rpki::publication::config_elt, 177
rpki::up_down::base_elt, 284
rpki::up_down::certificate_elt, 287
rpki::up_down::class_elt, 291
rpki::up_down::class_response_-syntax, 294
rpki::up_down::issue_pdu, 301
rpki::up_down::message_pdu, 309
rpki::up_down::revoke_syntax, 318
rpki::xml_utils::base_elt, 371
rpki::xml_utils::msg, 378
rpki::xml_utils::sax_handler, 381
startElementNS
rpki::xml_utils::sax_handler, 381
state
rpki::rpki_engine::ca_detail_obj, 248
status
rpki::up_down::error_response_pdu, 299
suggested_sia_head
rpki::up_down::class_elt, 292
sundial.py(1873), 394
sweep
rpki::sql::session, 268
symmetric_difference
rpki::resource_set::resource_set, 214

table
rpki::sql::template, 276
test
rpki::sundial, 49
test1
rpki::resource_set, 45
test2
rpki::resource_set, 45
text
rpki::xml_utils::sax_handler, 382
thisUpdate
rpki::manifest::Manifest, 164
tlslite
rpki::x509::RSA, 352
rpki::x509::X509, 363
tlslite::api::Checker, 383
tlslite::api::HTTPTLSConnection, 384
tlslite::api::TLSSocketServerMixIn, 384
tlslite_certChain
rpki::https, 35
to_DER
rpki::x509::PEM_converter, 341
to_PEM
rpki::x509::PEM_converter, 341
to_resource_bag
rpki::up_down::class_elt, 291
to_resource_range
rpki::resource_set::roa_prefix, 227
to_resource_set
rpki::resource_set::roa_prefix_set, 233
to_rfc3779_tuple
rpki::resource_set::resource_range_-as, 204
rpki::resource_set::resource_range_-ip, 206
rpki::resource_set::resource_set_as, 216
rpki::resource_set::resource_set_ip, 220
to_roa_tuple
rpki::resource_set::roa_prefix, 228
rpki::resource_set::roa_prefix_set, 233
to_sql
rpki::sundial::datetime, 280
rpki::x509::DER_object, 339
toASN1tuple
rpki::sundial::datetime, 280
toGeneralizedTime
rpki::sundial::datetime, 280
totimestamp
rpki::sundial::datetime, 280
toUTCTime
rpki::sundial::datetime, 280
toXML

rpki::left_right::list_resources_elt, 126
rpki::publication::publication_-object_elt, 191
rpki::up_down::certificate_elt, 287
rpki::up_down::class_elt, 291
rpki::up_down::class_response_-syntax, 294
rpki::up_down::error_response_pdu, 298
rpki::up_down::issue_pdu, 302
rpki::up_down::list_pdu, 305
rpki::up_down::message_pdu, 309
rpki::up_down::revoke_syntax, 318
rpki::xml_utils::base_elt, 371
rpki::xml_utils::data_elt, 376
rpki::xml_utils::msg, 378
toXMLtime
rpki::sundial::datetime, 280
trace
rpki::log, 38
type
rpki::up_down::message_pdu, 310
rpki::xml_utils::msg, 378
type2name
rpki::up_down::message_pdu, 310

undersized
rpki::resource_set::resource_bag, 199
unimplemented_control
rpki::left_right::data_elt, 122
rpki::xml_utils::data_elt, 376
union
rpki::resource_set::resource_bag, 199
rpki::resource_set::resource_set, 214
unwrap
rpki::x509::XML_CMS_object, 367
up_down
rpki::relaxng, 43
up_down.py(1873), 394
up_down_handler
rpki::rpki_engine::rpkid_context, 264
update
rpki::rpki_engine::ca_detail_obj, 246
rpki::sql::template, 276
update_children
rpki::left_right::self_elt, 157
update_roa
rpki::left_right::route_origin_elt, 148
update_roas
rpki::left_right::self_elt, 158
uri
rpki::rpki_engine::child_cert_obj, 257
uri_tail
rpki::rpki_engine::child_cert_obj, 257
uri_to_filename
rpki::left_right::repository_elt, 142
rpki::publication::publication_-object_elt, 191
use_hsm
rpki::left_right::self_elt, 159
use_pubd
rpki::left_right::repository_elt, 143
username
rpki::sql::session, 269

v4
rpki::resource_set::resource_bag, 200
v6
rpki::resource_set::resource_bag, 200
valid_until
rpki::left_right::list_resources_elt, 127
rpki::resource_set::resource_bag, 200
verify
rpki::x509::CMS_object, 326
version
rpki::left_right::msg, 129
rpki::left_right::sax_handler, 152
rpki::manifest::Manifest, 164
rpki::publication::msg, 186
rpki::publication::sax_handler, 197

rpki::roa::RouteOriginAttestation, 241
rpki::up_down::message_pdu, 310
rpki::up_down::sax_handler, 321
rpki::xml_utils::msg, 378

warn
rpki::log, 39
wired_in_config_id
rpki::publication::config_elt, 178
withdraw
rpki::left_right::repository_elt, 142
withdraw_roa
rpki::left_right::route_origin_elt, 149
wrap
rpki::x509::XML_CMS_object, 367

x509.py(1873), 395
x509store
rpki::https::Checker, 100
x509store_thunk
rpki::https::Checker, 99
xml::sax::handler::ContentHandler, 385
xml_utils.py(1873), 396
xmlns
rpki::left_right::left_right_-namespace, 124
rpki::publication::publication_-namespace, 188
rpki::up_down, 50